Human and organizational aspects of cyber security

From a System Suppliers Perspective

Muhammad Afzal

KTH Electrical Engineering

Master Thesis
Stockholm, Sweden 2010

XR-EE-ICS 2010:013

MASTER THESIS

HUMAN AND ORGANIZATIONAL ASPECTS OF CYBER SECURITY

From a System Suppliers Perspective

Department of Industrial Information and Control Systems
Royal Institute of Technology
Stockholm, Sweden

March, 2010

Contact Information:

Authors:
Muhammad Afzal
E-mail: mafz@kth.se, afzalchaudary@gmail.com

University advisors:
Teodor Sommestad
Industriella informations- och styrsystem
Osquldas väg 12, 7 tr SE-100 44 Stockholm
E-mail: TeodorS@ics.kth.se

ABSTRACT

SCADA systems have been successfully implemented in industries like oil, gas and electricity for maintenance, monitoring and control. While these systems provide immense advantage in terms of productivity, management and performance, they are also prone to exploitation and problems.

These SCADA systems largely consist of network infrastructure which is subject to cyber security issues. Most of the weaknesses, or threats posed to these systems can be eliminated or reduced if the human aspect associated with them can be explored and corrected if needed. Because of human involvement in planning, designing, developing, deployment and operating of such systems, probability of flaws will always be present.

This study focuses on such human aspects which effect cyber security in SCADA systems. We identified common mistakes which can be attributed to human error or negligence. A set of causes was then identified by use of interviews and finally, a Bayesian model was developed to simulate the identified cases and mistakes. We analyzed the influence and probability of occurrence of mistakes using this model.

Our results prove that causes of the mistakes resulting in security problems for SCADA systems are directly related to human aspects. Furthermore, we identified some of the most prominent of these causes in this study. Based on the identified causes and mistakes, we suggested mitigation strategies to cater the problems faced.

ACKNOWLEDGEMENT

First and foremost, I would like to express our sincere and heartfelt gratitude to our Thesis Supervisor, Mr. Teodor Sommestad, for taking the time, effort and patience to provide me with her invaluable guidance, comments and encouragement to complete this project. His extensive discussions and knowledge around this work have been very helpful for this study.

I am thankful to all experts who gave me time for interviews and guide me patiently with their feedback and support through this project. Their supervision and constant encouragement motivate me to give my best for the better outcome.

I would also like to thank my thesis colleague for motivating me in every stage of this thesis.

My friends and family
Thank you.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

KTH - *Kungliga Tekniska Högskolan*
ICS - *Industrial Information and Control Systems (ICS)*
SCADA -*Supervisory Control and Data Acquisition*
DNP - *Distributed Network Protocol*
TCP - *Transmission Control Protocol*
IP - *Internet Protocol*
IDS - *Intrusion Detection System*
DMZ - *Demilitarized Zone*
DOS - *Denial-of-Service*
DDOS - *Distributed Denial-of-Service*
UID - *User Identifier / Identification*
BN - *Bayesian Networks*
CPT - *Conditional Probability Table*
IEEE - *Institute of Electrical and Electronics Engineers*
IEC - *International Electrotechnical Commission*
NIST - *National Institute of Standards and Technology*
CSD - *Computer Security Division*
US CERT - *US State Computer Emergency Readiness Team's*
CSSP - *Control System Security Program*
INL - *Idaho National Laboratory*
CPNI - *Center of the Protection of National Infrastructure*
NASCIO - *National Association of State Chief Information Officers*
OECD - *Organization for Economic Co-operation and Development*
NCS - *National Communications System*
PITAC - *President's Information Technology Advisory Committee*
NITRD - *Networking and Information Technology Research and Development*
ISPs - *Internet Service Providers*
OS - *Operating System*
AP - *Access Point*
SW - *Software*
IS - *Information System*
IRC - *Internet Relay Chat*
WLAN - *Wireless Local Area Network*
P2P - *Peer-to-Peer Computer Network*
WWW - *World Wide Web*
DNS - *Domain Name Server*
DMA - *Direct Memory Access*
DoS - *Denial of Service*
ACL - *Access Control List*
IDS - *Intrusion Detection System*
ARP - *Address Resolution Protocol*
VPN - *Virtual Private Network*
IOS - *Internetwork Operating System*
URL - *Uniform Resource Locator*
ICT - *Information and Communication Technology*
PDAs - *Personal Digital Assistant*
MAC - *Media Access Control*
FIPS - *Federal Information Processing Standards*
EAP - *Extensible authentication Protocol*
CPU - *Central Processing Unit*
HP - *Hewlett-Packard*

1 INTRODUCTION

Growing interconnectivity of SCADA system has exposed them to a wide range of security risk due to unwanted behaviors of users and administrators and other technical staff involved in operation Human factor is the biggest security flaw[1] and it is important for supplier and customers to mitigate it.

- *"The most frequently mentioned sources of security vulnerability in computer networks are poor security management and incorrect implementation"* [2]
- *"Perhaps the biggest challenge that any organization faces when it comes to network security is human error. Kaeo said many organizations don't even take the simple step of creating unique and complex passwords" "Unbelievable as it may be, a lot of passwords are just 'Cisco,'" she said. "That is inexcusable"* [3].

History demonstrates trust on an advance technology is damned if the people operating the system are not fully disciplined and managed [4]. Failure in system functions often occurs due to untested and improper configured systems[5], [6].

This document will cover aforementioned and other similar points under the subject of "Human and Organizational Aspects of Cyber Security" as Master´s Thesis, proposed by Industrial and Information Control Systems Department of KTH.

2 BACKGROUND

This chapter provides the overview of SCADA (Supervisory Control And Data Acquisition) systems. The types and purpose of computer server machines and network devices.

Control system is one of the most complex systems to be managed and operated. This is because of their size, dynamic nature and the large amount of various components and entities.

SCADA systems are spread on large geographical scale, connected through different medium. A variety of communication networks are interconnected to the electric grid for the purpose of sensing, monitoring, and controlling. Different SCADA components, e.g. field devices, acquisition systems etc. , are part of critical infrastructure such as power plants, substations, energy control centers, company headquarters, regional operating offices, and large load sites. These devices and systems are increasingly networked and complex [9]

These systems are protected with firewalls, multiple authentication systems, authorization schemes, physical access control systems etc. A system which appears to be technically secured in accordance with best practices can still be vulnerable to attacks due to human mistakes. Misconduct, stress, sloppiness, negligence or incompetence from humans related to the system may compromise intended security functionality or introduce new, unwanted, functionality into the system [10].

If SCADA system compromised it can result in no water generation, no fuel supply, and no electricity in public as well as private sectors. Often administrators who are responsible to install, configure and manage such system are not taking care of all steps that must be concerned in it [10].

This document, hopefully, would offer some useful suggestions to the mentioned research issues. It will describe the general mistakes and causes due to the negligence of engineers involved in installation, configuration, maintenance and operations.

2.1 SCADA

SCADA system are those which gather data from remote sites and transmit collected data to central site for operator´s observation. The collected data is usually viewed on one or more SCADA host computers located at central site. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station controllers, known as field devices. Power industry is among those which rely on SCADA systems. With the help of SCADA engineers are able to gather information about

system operation as well as assist regulate and control power generation. SCADA systems are composed of numerous Server, Workstation, Communication Links, Field devices and Network Devices as shown in Figure 1.

Authentication Server manages users´ access to system whereas the application server is to executing real-time data and operations. Application Server is also responsible of exchanging data with other control center. The job of Frontend Server is to collects data from process, forward commands and set points to control the process. Historians are servers dedicated to supervise historical information and calculations of historical data. The Database Server serves as data storage and retrieval. Web server and Antivirus server manage HTTP connections and malware prevention respectively.

System operator use Workstations as there control stations. These consist of software interfaces to communicate with different SCADA components. Such software presents large amounts of data to the operator, which represents the current state and activity of the system in the form of events and alarms.

Field devices are typically found in remote sites of SCADA networks such as pumping plants, substations, electric motors or turnouts. These are connected with the SCADA network through RTUs and switches. The network devices such as switches, routers, firewalls etc. are manage communication and access control in SCADA network.

SCADA Control System Overview

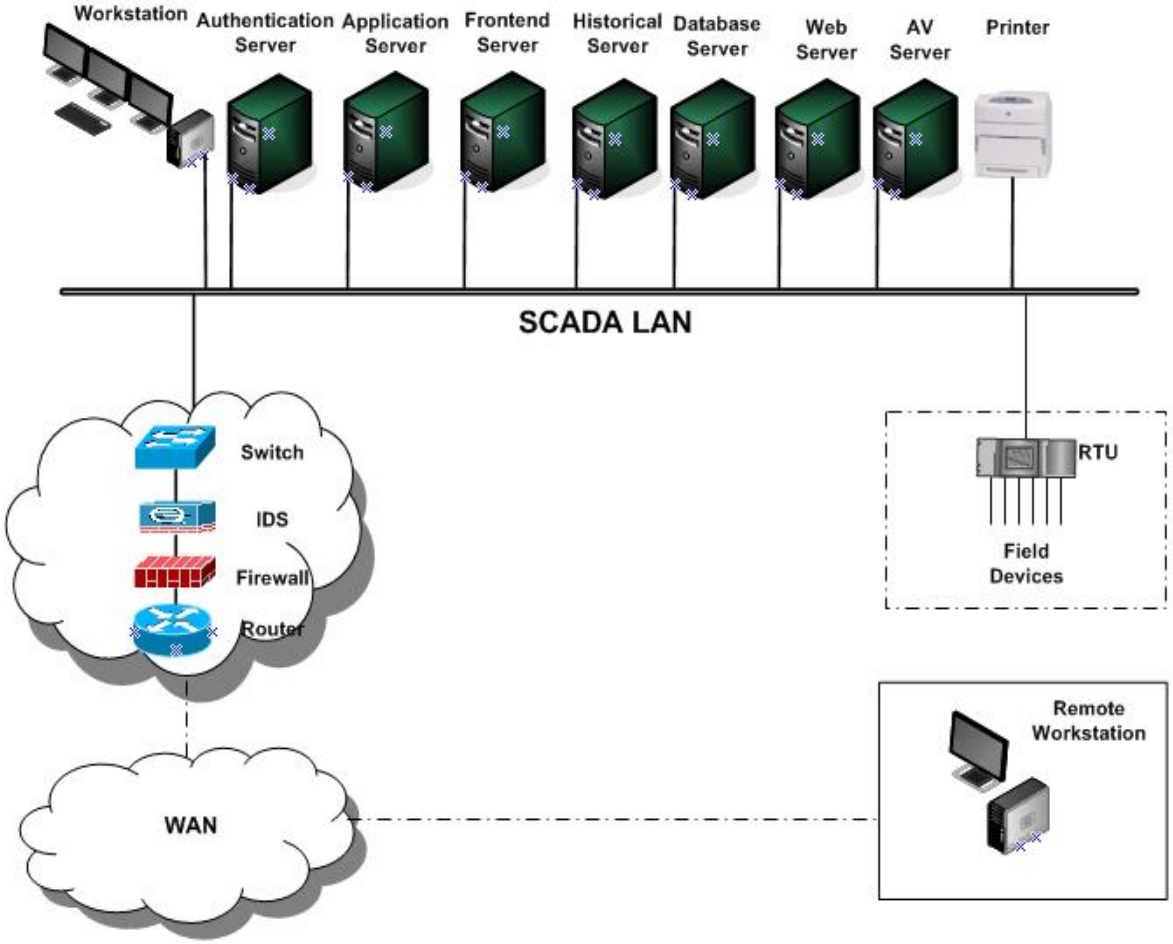

Figure 1 - SCADA Control System Overview

3 RESEARCH PURPOSE, PROBLEMS AND GOALS

This chapter explains the project purpose, problem domain, project goals and the research question. Reader will be given an understanding of why SCADA cyber security is crucial and why the requirement of its improvement is felt.

3.1 Project Purpose

The objectives of this project are:

- To identify vulnerabilities and causes because of human negligence respective of installation, configuration, operation and management in SCADA system.
- Scale them with respect to the potential damage possibly caused by their vulnerability exploitations, and countermeasure suggestions against those vulnerabilities.

3.2 Problem Domain

Seeking technological improvements in SCADA system to prevent cyber attack is important. The processing, controlling, maintenance and configuration of such system depend on human initiated actions, so prevent users from making awful decisions is difficult. When the individuals involved in operation expose system to threats because of negligence, the collection of these makes it dangerous for entire project.
The System Administrators and/or operators may introduce vulnerabilities in system due to the inaccurate installation and configuration of antivirus, firewalls, IDS etc. Other cases of incorrect security implementations include failure to use auditing functions, examination of existing log files, granting unnecessary access rights, failure to review access rights at regular intervals, multiple assignment of the same log-in name, inappropriate process management, existence of unnecessary open ports and unused services, carelessness to monitor in/out traffic, analyze implementation of weak password policy [7] and failure to use the available security tools [11]. In case of poor configuration of the network components, the availability of entire network can disrupt, furthermore confidentiality and integrity of data can be impaired. For example an unnecessary program at system boot up could leave system open for cyber attack. Hence there is a need of careful configuration, maintenance and operation of installed systems

3.3 Goals

Human and organizational behavior plays key role in security of an organization.
Main goals of this thesis are

- Identifying unwanted behaviors that users and administrators can have.
- Identify the ways for such behaviors that can influence the cyber security, study vulnerabilities and security gaps that can be occurs due to such kind of behaviors
- Identifying the behavior of the Administrator and/or Operators to ensure SCADA operation are being completed properly
- If time and opportunity are available, research and test possible mitigation techniques as part of a mitigation strategy

3.4 Research Questions

Criminals and hackers repeatedly deceive users to malwares exposure against their computers and connected networks.
Users and/or administrator have been expressed as the weakest link in security scheme [12] because of their behavior. For example countless studies have shown that users be likely to choose short and/or guessable passwords.

Possibly the most severe behavioral problem of system Administrators and Engineers is poor configuration of the system. This may be caused by failure to realize the security technology, or failure to follow the correct procedures [11]. Another problem seen is poor operating procedures e.g. not keeping the system up-to-date, not responding to security notices, poorly managing authentication and authorization schemes, and laziness.

Considering aforementioned facts in mind, following questions can be raised:

- What are the main mistakes for security being compromised in automation control systems?
- What are the main causes of these mistakes?
- What should be done to mitigate these causes?

4 METHODOLOGY

This chapter explains the general methodology adopted and research methods used in the project to gather the possible mistakes and the causes of such mistakes.

The project's aim was to find out and mitigate mistakes along with their causes that influence installation, configuration and management of computer networks, operating system and SCADA[1] applications. The first task was to identify the variables that are of importance, along with their possible values. These variables were essentially the mistakes committed by the administrators and engineers along with their causes. The important task here was to elicit the variables of importance as well as the relationships between these variables.

To achieve this task, the adopted methodology was divided into two main parts. The first part consisted of literature studies to identify mistakes. Appendix A (Section 10.1.1) provides list of these mistakes.

The second part was a set of interviews comprising of three phases which were based on the identified mistakes. These phases are shown in Figure 2. Interviews were used because these are the most common method of attaining probabilistic information. Although other sources are available which provide these information but they do not always have all the numbers required for the quantitative part of a probabilistic network [17]. The purpose of these interviews was to:

1. Phase I – List of possible causes for each of the mistakes identified earlier.
2. Phase II – The probability of the causes identified in Phase I.
3. Phase III – Conditional probabilities of mistakes based on the causes.

See Appendix A, Section 10.1.2 Questionnaire PHASE I, for list of causes. The data from these three phases were used to calculate the influence of each of the causes on the mistakes and the relationships between them.

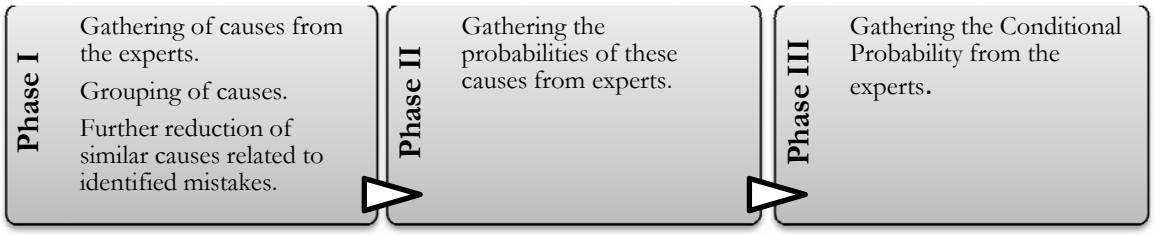

Figure 2 - Interview Phases

The outcome of the literature studies and the three phase interviews were a set of data expressing mistakes, their causes and probabilistic values of the measure of their influence. This data were used to create a Bayesian Network for verification and analysis.

[1] SCADA stands for supervisory control and data acquisition. It generally refers to an industrial control system, a computer system monitoring and controlling a process

Bayesian Network is a graphical model to represent the relationships between variables. We used this gphical model for analysis as this method supports a complete and intuitive description of decision problems, stating both what is desired and what alternatives are available [15]. The data from the three phases were used in building a Bayesian Network. This was done to find the probabilities of each of the variables.

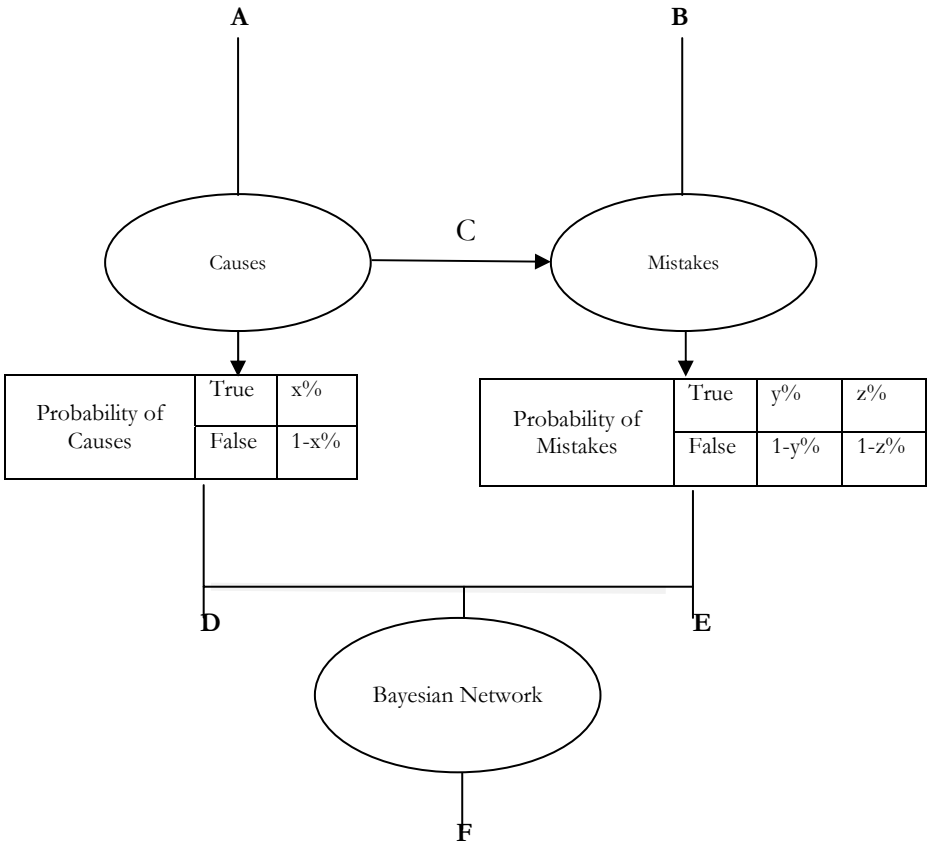

Figure 3 - Research Method Overview

Figure 2, depicts the methodology for this process. As shown in Figure 3, "A" (Causes) comes from experts during interview, "B" (Mistakes) comes through literature study. "C" shows the influence of causes to mistakes. "D" and "E" (probability in numbers) comes from experts during face to face interview and "F" (Bayesian Network) has been modeled in GeNIe[2].

In the following sections we start with a subset of our problem, as an example, to introduce Bayesian Networks. And then the complete process is explained in detail.

[2] GeNIe is a development environment for building graphical decision-theoretic models

4.1 Bayesian Networks

A Bayesian network is a graphical model that encodes probabilistic relationships among variables of interest [16]. For example, a Bayesian network could represent the probabilistic relationships between diseases and symptoms. Given symptoms, the network can be used to compute the probabilities of the presence of various diseases.
Bayesian Networks have been widely used in problem domains where the number of variables is indefinite and so are their values. Taking binary approach to figure out an outcome hasn't always been applicable e.g. the possibility of firewall misconfigurations defined as 0, as in impossible or 1, as in possible.

For instance, in the outcomes for firewall misconfigurations, assume the amount of variables involved behind these outcomes such as how much resources organizations have, how well knowledge administrator have, how much complex configuration could be etc [15]. A Bayesian Network for this example is shown in Figure 4.

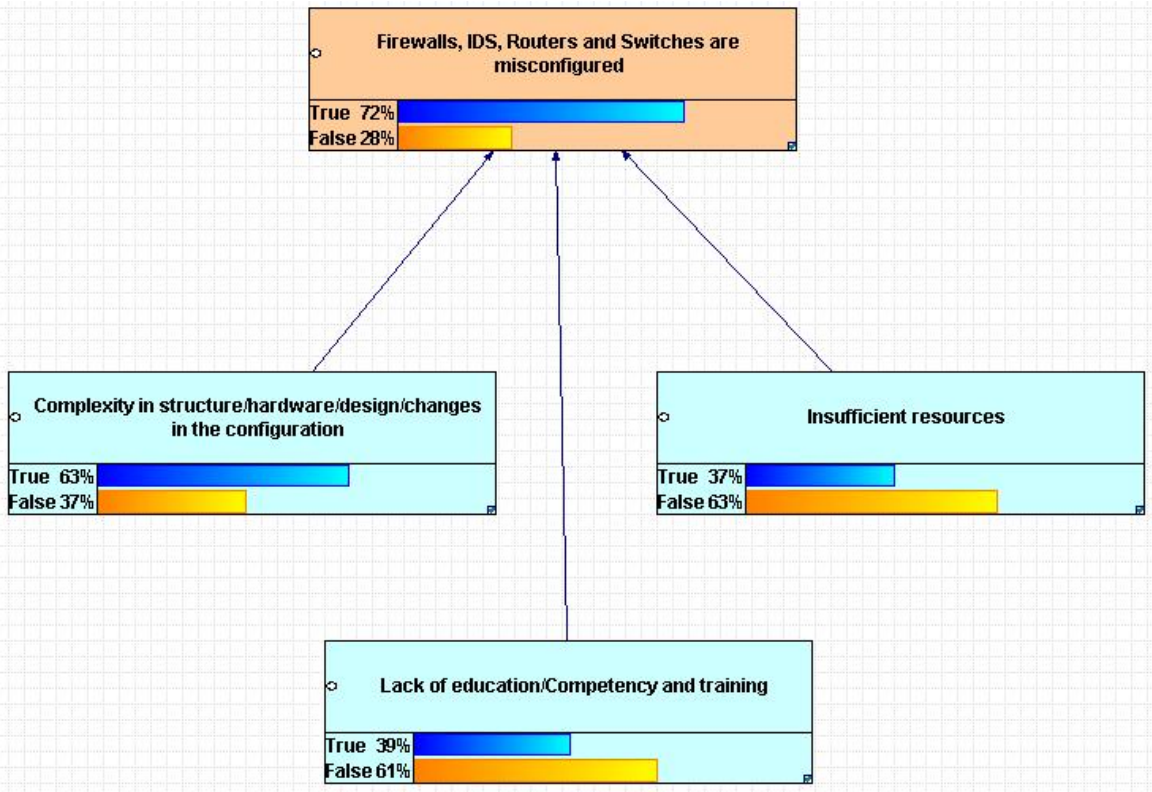

Figure 4 - Example Working of Bayesian Network

In the Figure 4 probability that a Firewall is misconfigured depend on the conditions (e.g. if the project is delivered under work stress). To define how these causes influence the probability one would have to set the attributes in the CPT[3]. In other words, for each combination of these causes a probability that a Firewall is misconfigured. i.e. P(Firewall misconfigured = True $|Factor_1,. ., Factor_N$). In given example, 8 (2^N) probabilities need to be asked from the respondent (to get the 16 probabilities).

There can, however, be numerous factors that influence these mistakes. To gather and then to reduce these causes we iteratively interviewed, to come up with a compact and precise list of mistakes. First causes of misconfigured Firewall have been collected and obtain a long list of respondent opinions. Then the list was

[3] The number of probability distributions required to populate a conditional probability table (CPT)

ordered and the main causes for each type of mistake identified. Finally most relevant causes were chosen to reduce the size of CPT. These dimensionality reduction were necessary, else there would be a numerous factors for a respondent to answer, as well to remove repetition.

Experts were asked to specify a numeric value for probability distribution over a variable's (let's call it V) states. So we can say, what is the probability of causes being "True" and "False" respectively. Probability distribution is influenced by given factors (say A1, A2 and A3). In given example, arrow has been drawn from the factors that influence the variable. Hence, from A1, A2 and A3 to V

The Table 1 was produced from GeNIe[4]. It shows the different states for each combination of different factors. Each variable can be in True of False state. So there will be 8 different combinations, as discussed above.

Table 1 - Conditional Probability Table

	(A1) Complexity in Structure	T				F			
	(A2) Insufficient Resources	T		F		T		F	
	(A3) Lack of Education	T	F	T	F	T	F	T	F
(V) Firewall Misconfigured	True	P1	P2	P3	P4	P5	P6	P7	P8
	False	1-P1	1-P2	1-P3	1-P4	1-P5	1-P6	1-P7	1-P8

The questions asked to experts, in this case, were the probabilities P1 to P8. These represent a probability for V being "True" given A1, A2 and A3 are in a certain states. So for example, P2 should be the probability P(V=True | A1=True, A2=True and A3= False). In clear text: "How probable is it that V is True if A1 is True, A2 is True and A3 is False).

Hence we get, for all possible combinations of states for given factors that influence V, what is the probability that V is True. The probability for V is False can be calculated by taking difference of 1.

P1 should be the probability P(V=True | A1=True, A2=True and A3= True)

P2 should be the probability P(V=True | A1=True, A2=True and A3= False)

P3 should be the probability P(V=True | A1=True, A2=False and A3= True)

P4 should be the probability P(V=True | A1=True, A2=False and A3= False)

P5 should be the probability P(V=True | A1=False, A2=True and A3= True)

P6 should be the probability P(V=True | A1=False, A2=True and A3= False)

P7 should be the probability P(V=True | A1=False, A2=False and A3= True)

P8 should be the probability P(V=True | A1=False, A2=False and A3= False)

[4] GeNIe is a development environment for building graphical decision-theoretic models

4.2 Mistakes Identified from Literature Studies

The cyber security aspect of SCADA systems has been widely discussed in books, publications, seminars and whitepapers. The same were used to collect probable mistakes to attain project's objectives. These mistakes are discussed in detail in section 6 of this report. The source of this information was several institutions working on related issues. A list of these institutions is presented as Appendix B Section 11.1, to this report.

These institutions were chosen due to their work done in cyber security of control systems including SCADA. They continuously publish latest threats, probable mistakes leads to vulnerabilities, reports and articles on relevant scope. These publications include common vulnerabilities existing in SCADA systems, best practices to eliminate those vulnerabilities or at least make them hard for the attackers to exploit and so forth. This data significantly helped in identification of mistakes and preparing questionnaires. These also helped to get the knowledge from experts about human negligence of installation, configurations, operations and management of computer network and SCADA Applications. List of mistakes identified in this phase, and questionnaire based on them are listen in Appendix A, List of Mistakes. A series of interviews were conducted using this questionnaire.

4.3 Interviews and Data Analysis Phase

On the basis of mistakes, interviews with the experts were conducted to get the probable list of causes. This is primarily common method to get probabilistic information [17]. Hard copy of questionnaire was presented during a face-to-face interview.

The experts include, Managers (those are involved in all phases of project), Security Experts (responsible for cyber security in SCADA system) and System Engineers (responsible of installation, configuration and management of the SCADA system). It was important to reach all these personnel to find the causes of probable mistakes made at some point in the projects since Managers who are involved in different projects from start till shipment have their own expert opinion. Security experts on the other hand, design security policies. System Engineers are involved in operation and implementation of the designed policy on system. They have their own observations on system's efficiency or deficiency in response to the new policy.

There were a total of eight experts within the same organization, who took part in the interview. Of all the participants there were seven male and one female. They were between 30 and 60 years old. All experts were from engineering background with extensive experience in SCADA system. The profile of experts has been explained under section 4.3.1.

4.3.1 Experts Profile

Sr. No	Designation	Experience (SCADA System)	Expertise
Respondent A	Line Manager Applications	33 year	SCADA and communication system
Respondent B	Manager System Engineering	30 year	System integration and technical project management. Software development process, customer requirements, test procedures and integration.
Respondent C	System Engineer	25 year	System design and architecture. Installation, configuration and management of operating system. Communication network

			configuration. Hardware assembling.
Respondent D	Security Expert	20 year	System architecture and cyber security.
Respondent E	Plant Engineer	10 year	Installation and configuration of operating system as well as SCADA Applications System.
Respondent F	Service Manager	30 year	He has extensive knowledge of SW engineering, project management including R&D management.
Respondent G	Manager Plant Engineering	40 year	Expert in engineering services, SCADA system and also teaching SCADA system.
Respondent H	Technical Project Manager	25 year	System integration and technical project management. He is also involved in software development process, customer requirements, test procedures, function commissioning on site and Integration testing, FAT, SAT

4.3.2 Phase I – Gathering Causes of Mistakes

Questionnaires for Phase I were prepared keeping in mind the mistakes that occur. These questionnaires together with interviews with the experts were used to gather factors that resulted in these mistakes. The Factors/Causes of mistakes were open ended answers to the questions by the experts depending upon what they thought were the reasons of mistakes. A total of 15 questions were identified and used during the interviews to identify causes of mistakes. Due to the open nature of question, the answers vary from one expert to another but were similar in nature. A reduction was later applied to extract common/key factors from these collected data. For the complete list of causes for all mistakes see Appendix A-Section 10.1.2 Questionnaire Phase I, List of Causes.

4.3.2.1 Grouping of Similar Causes

As mentioned above, this step was done to remove repetition and reduce the number of causes that will be used in the next phase of interviews. The number of causes was too many to be used in Bayesian Network as a method of analysis. So these causes were reduced to a homogenous taxonomy, merging those that are similar and prioritizing which to include.

For instance the causes of Firewalls, IDS , Routers and Switches misconfigurations could be "**low level education**" , "**lack of education**", "**Insufficient training**" and "**lack of competency**". So we can say it is "**Lack of education/Competency and training**", instead of four causes, discussed above. See Appendix A, Section 10.1.3 Questionnaire Phase I, Grouping of similar causes for detailed procedure to identify how causes have been reduced. Once all causes were grouped, they were validated with some of the experts and recommended modifications were made so the causes were accurately grouped.

Once the common causes have been identified, by reducing the similar ones as explained above, they were drawn as a Bayesian Network to show their influence on one or more mistakes. One cause may influence several mistakes. The arrows in Figure 5 below show possible relationship between causes and mistakes.

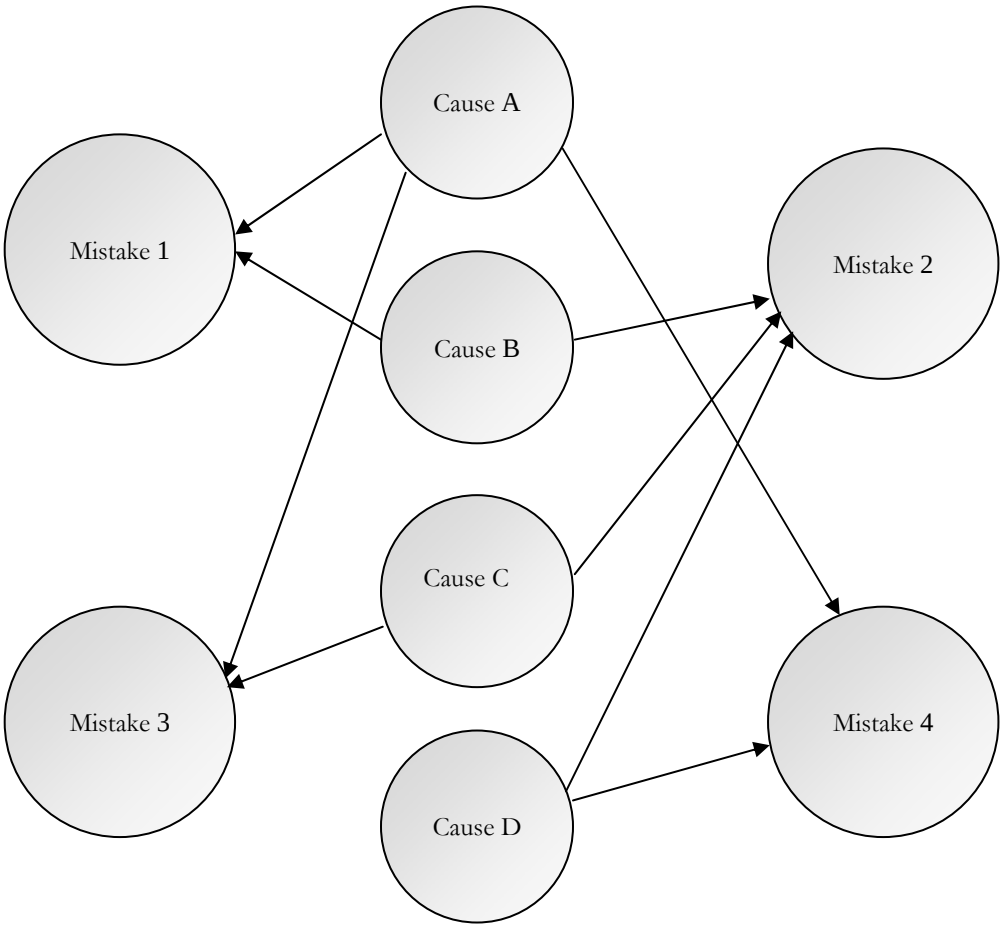

Figure 5 - Model Consist of Mistake and Causes.

4.3.3 Phase II – Probabilities of Causes

The first phase of interview gave us the common causes. This information, though, valuable was not sufficient to be used in Bayesian Network. So we consulted with the experts in the second phase of interview, to gather numeric values for the severity of these groups of causes. Table 2 shows a sample questionnaire prepared and presented during interview with experts. The values suggested by the experts were compiled, and the average was calculated to be used in causes nodes in Bayesian Network as shown in Figure 6.

Table 2 - Probability of causes

Causes Groups	Probabilities						
	Respondent-A	Respondent-B	Respondent-C	Respondent-D	Respondent-E	Respondent-F	Average
Cause A	PA_1	PA_2	PA_3	PA_4	PA_5	PA_6	$PAavg = \frac{\sum_6^1 P}{6}$
Cause B	PB_1	PB_2	PB_3	PB_4	PB_5	PB_6	$PBavg = \frac{\sum_6^1 P}{6}$
Cause C	PC_1	PC_2	PC_3	PC_4	PC_5	PC_6	$PCavg = \frac{\sum_6^1 P}{6}$
Cause D	PD_1	PD_2	PD_3	PD_4	PD_5	PD_6	$PDavg = \frac{\sum_6^1 P}{6}$
…	…	…	…	…	…	…	…

On the basis of probabilities from the experts, we were able to rank the causes. This showed the severity level of each cause in general. Since these values alone did not show the measure of influence of each cause to its relevant mistake, the values for conditional probability were gathered in Phase III discussed in section 4.3.6 below. These rankings, however, were obtained to provide the sorted list of causes for each mistake to the experts. See Appendix A, Section 10.2 Questionnaire Phase II, Priority/Ranking of Cause.

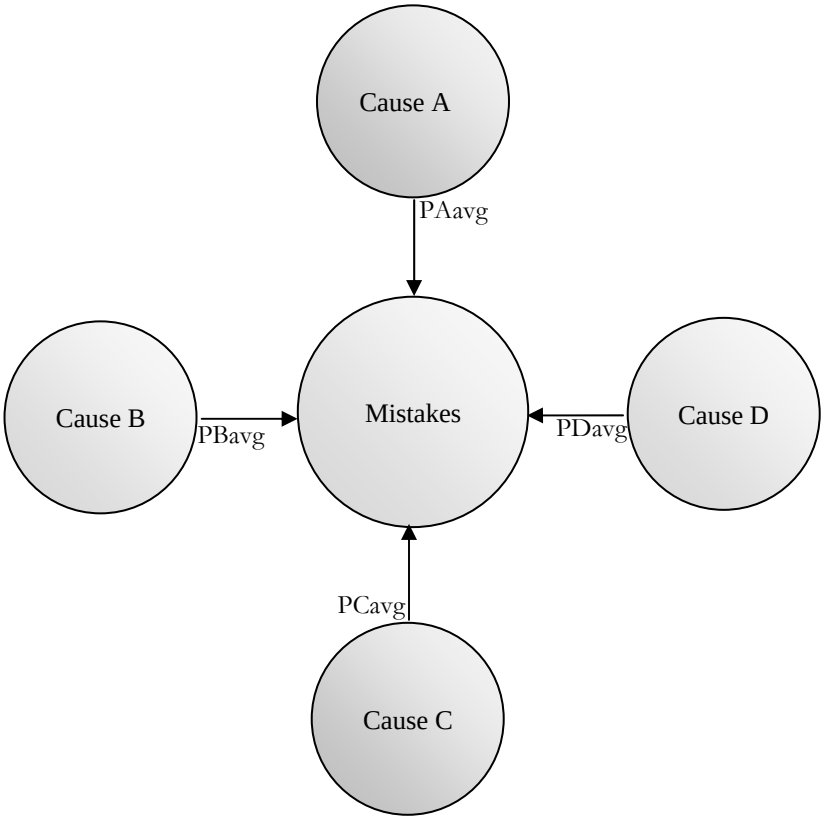

Figure 6 - Probabilities Placed in Causes Nodes

4.3.4 Phase III – Probability of Mistakes Using Conditional Probability Table

The earlier phases of interview, gave us the probable causes for identified mistakes. This information, though valuable, is not sufficient to predict any meaningful mitigation plan against the mistakes. So we consulted with the experts, in the third phase of interview to gather numeric values for probability distribution of the mistakes.

In this final phase of interview, following questionnaire based on CPT[5] was prepared to get the severity of influence of causes for each mistake. Table 3 below is an example of questionnaire presented while meeting with experts. The experts with different backgrounds were interviewed to obtain probabilities (Px1 – Px16 where x denotes a particular expert's values) used for CPT. Fifteen tables were produced simultaneously to attain the probability of mistakes. The CPT calculation procedure is explained in section 4.1.

After the probability of these variables was acquired from the experts, the mean value was calculated. To ensure the difference between values obtained from the experts Mean Absolute Deviation (MAD) was estimated. It gives the average of the absolute deviations and is a summary of statistical dispersion or variance. It was noticed that there is insignificant variation between the values taken from the experts. See Appendix A, Section 10.3 Questionnaire Phase III, CPT for detailed observation of mean value and MAD calculations in CPT.

This phase took most of the time since it was difficult to get time from the experts to fill questionnaires on so many causes and their probabilities. Once interviews were completed, the process of compilation and placing the probabilities in Bayesian Network was finalized.

Table 3 - Conditional Probability Table Calculations

Variable Mistake — Variable Causes — Conditions

	(Cause A) Complexity in structure/hardware/ design/changes in the configuration	T								F									
	(Cause B) Lack of requirements engineering/poor documentation	T				F				T				F					
	(Cause C) Lack of education/Competency and training	T		F		T		F		T		F		T		F			
(Mistake 1) Firewalls, IDS, Routers and Switches are misconfigured?	**(Cause D)** Insufficient resources	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
Respondent-A	TRUE	PA_1	PA_2	PA_3	PA_4	PA_5	PA_6	PA_7	PA_8	PA_9	PA_{10}	PA_{11}	PA_{12}	PA_{13}	PA_{14}	PA_{15}	PA_{16}		
Respondent-B	TRUE	PB_1	PB_2	PB_3	PB_4	PB_5	PB_6	PB_7	PB_8	PB_9	PB_{10}	PB_{11}	PB_{12}	PB_{13}	PB_{14}	PB_{15}	PB_{16}		
Respondent-C	TRUE	PC_1	PC_2	PC_3	PC_4	PC_5	PC_6	PC_7	PC_8	PC_9	PC_{10}	PC_{11}	PC_{12}	PC_{13}	PC_{14}	PC_{15}	PC_{16}		
Respondent-D	TRUE	PD_1	PD_2	PD_3	PD_4	PD_5	PD_6	PD_7	PD_8	PD_9	PD_{10}	PD_{11}	PD_{12}	PD_{13}	PD_{14}	PD_{15}	PD_{16}		
Respondent-E	TRUE	PE_1	PE_2	PE_3	PE_4	PE_5	PE_6	PE_7	PE_8	PE_9	PE_{10}	PE_{11}	PE_{12}	PE_{13}	PE_{14}	PE_{15}	PE_{16}		
Respondent-F	TRUE	PF_1	PF_2	PF_3	PF_4	PF_5	PF_6	PF_7	PF_8	PF_9	PF_{10}	PF_{11}	PF_{12}	PF_{13}	PF_{14}	PF_{15}	PF_{16}		

[5] The number of probability distributions required to populate a conditional probability table (CPT)

Respondent-G	TRUE	PG_1	PG_2	PG_3	PG_4	PG_5	PG_6	PG_7	PG_8	PG_9	PG_{10}	PG_{11}	PG_{12}	PG_{13}	PG_{14}	PG_{15}	PG_{16}
Respondent-H	TRUE	PH_1	PH_2	PH_3	PH_4	PH_5	PH_6	PH_7	PH_8	PH_9	PH_{10}	PH_{11}	PH_{12}	PH_{13}	PH_{14}	PH_{15}	PH_{16}
MEAN VALUE		Pavg1	Pavg2	Pavg3	Pavg4	Pavg5	Pavg6	Pavg7	Pavg8	Pavg9	Pavg10	Pavg11	Pavg12	Pavg13	Pavg14	Pavg15	Pavg16
MAD (Mean Absolute Deviation)																	

These conditional probabilities were put in the Bayesian model shown against each of the mistake nodes to obtain the final probability of occurrence of each of the mistakes. This conditional probability, as the name suggests, depends considerably on the conditions applied due to the absence or presence of one or more causes. This can be observed in the CPT shown in Table 3 above which depicts the absence or presence of causes in the form of a Truth Table. The mean of the probabilities provided by all the respondents is used as the final conditional probability to be used in the Bayesian Network as shown in Figure 7 below.

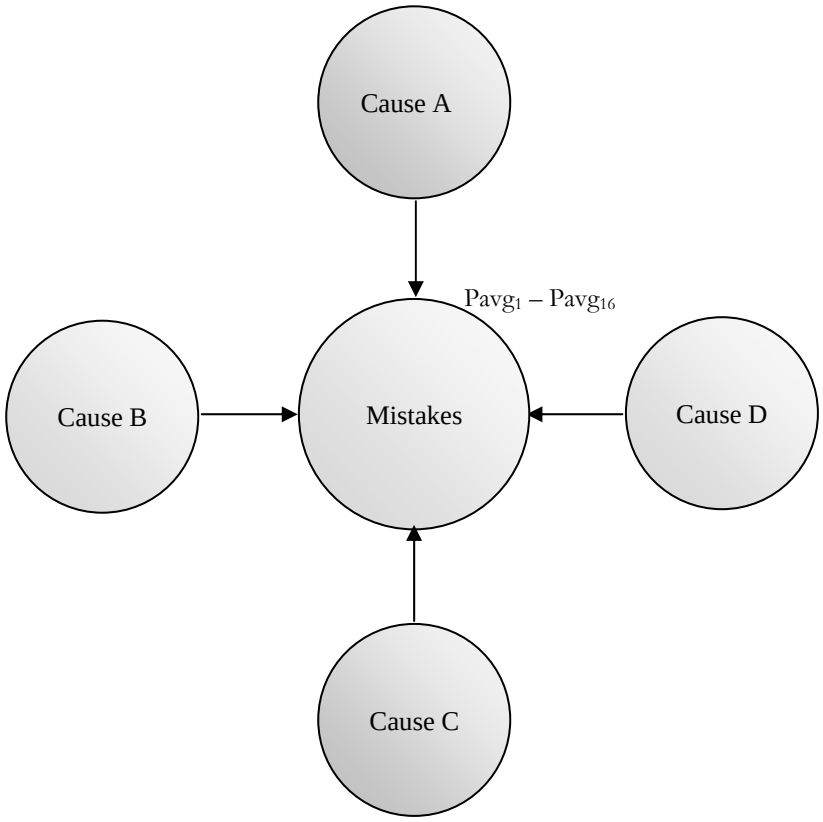

Figure 7 - Probabilities Placed in Mistakes Nodes

5 LITERATURE REVIEW - MISTAKES CAUSED BY HUMAN CARELESSNESS

This chapter presents the literature study results which are the identified mistakes committed during a project. Vulnerabilities, possible attacks and some case studies related to these mistakes are also discussed.

Vulnerabilities in corporate and/or SCADA networks are increasing rapidly due to the mistakes in installation, configuration, operation, testing, maintenance and management. Such mistakes may possibly provide a way for attacker to breach the System [18], [19]. The following section outlines several common mistakes that were identified during the literature review conducted in the beginning of this research.

5.1 List of Mistakes

This section describes the outcome of the literature studies as a list of probable mistakes found in an average project from a system supplier perspective. Based on this list a set of questions were produced to identify the causes of these mistakes. Following table shows mistakes identified during literature study.

Table 4 - List of Mistakes

Sr No	List of Doable Mistakes	Description
1	Firewalls, IDS, Routers and Switches are misconfigured.	Improperly configured firewalls could permit unnecessary data to pass between control and corporate networks. This could cause several problems including attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping and providing individuals with unauthorized access to systems. In such situation DOS, DDOS attack [27][108], Sniffer or Snooping [109] and Man in the Middle attacks [110] are possible.
2	Installation and configuration of operating system and software used in SCADA and/or corporate network are not completed correctly.	If the Operating System running SCADA applications are poorly configured and maintained, back doors could be exploited and Operating Systems can be compromised. Without a secured operating system, hackers can directly penetrate private internal networks or create attacks similar to Denial of Service. Spamming [22] and Man-in-the-middle attack [23],[25] is probable in such circumstances.
3	Unnecessary Ports and services left open after installation of operating system or application.	Network virus could enter through unprotected ports and compromise whole network. Denial of Service attacks [27] and flooding attacks [111] are possible.
4	Wireless Links in computer network are misconfigured.	If the authentication between wireless clients and access points is poorly configured or has weak security, the adversaries can deploy a

		rogue access point and connect to a control system's wireless network. Denial of Service, man in the middle, and ARP poisoning attacks [112] are possible. MAC Spoofing [113] and IP Masking [115] is also doable.
5	Default setting/values of devices are not changed during configuration.	Using default configuration or settings often lead to insecure and unnecessary open ports and exploitable network services running on hosts. By exploiting these security holes unauthorized access is possible.
6	System maintenance, modification and testing is not completed correctly.	Carelessness in the procedure of system configuration, maintenance, modifications and testing before, during, and after system implementation can lead to security oversights, exposures, and risks. DOS [27] and Man-in-the-middle attacks [110] are probable.
7	Access control policies in computer networks are in sufficient and not implemented correctly.	Unauthorized access to network devices and administrative functions could allow a user to disrupt control system operations or monitor network activity. Insufficient policies and procedures can give rise to threats. Spoofing Attack [7], [114] is possible.
8	Taking and restoration from backups are completed incorrectly.	If caution is not exercised in the process and procedures for the backup and restore, it can cause a failure of availability. Just in case backups are not available for immediate use to recover from a massive security incident, it can cause damage or stoppage in service [19].
9	Updates and Patches of OS, Antivirus and firmware are not managed properly.	If operating systems running the SCADA applications are not updated and maintained, the adversary can take benefit of vulnerabilities and attempt attacks such as spamming and viruses attack [118].
10	Supporting services or facilities not managed properly.	If there is no suitable procedure for supporting services for instance Uninterruptible Power Supply (UPS), battery backup and other equipment, it can cause damage or destruction and loss of availability [120].
11	Peripheral Devices are not managed properly.	Insecure universal serial bus (USB) and PS/2 ports could allow unauthorized connection of thumb drives, keystroke loggers, etc. Data theft and virus attack [19] are doable.
12	Strong password policy not implemented e.g. minimum password length, use of alpha-numeric and special characters	In most circumstances passwords not changed regularly or dictionary words are used, which can be broken to gain unauthorized access to the network. Such access could allow an adversary to disrupt control system operations or monitor its activity. Failure to comply with policy for strong passwords can lead to guessable passwords which are prone to Dictionary [78], Brute force [71] and Password

		Guessing attacks [117].
13	Password is written down on paper by user incase of strong password.	Typically users write password on key boards, desks etc. if strong password policy is implemented. This can lead to Eavesdropping [19]
14	Log management e.g. Proper Backup and reading of logs generated by system and devices is not completed properly.	Without proper and accurate logs, it might be impossible to determine what caused a security incident. Without regular log monitoring, incidents might go unnoticed, leading to additional damage and/or disruption. Regular log monitoring is also needed to identify problems with security controls, such as misconfigurations and failures.
15	Sensitive information from Technical Staff disclosed by means of social engineering.	By using social engineering [116] tactics it is possible to gain unauthorized access to systems or information in order to perform intrusion, identity theft, or simply to disrupt the system or network.

5.1.1 Firewalls, IDS, Routers and Switches are Misconfigured

Firewalls are the foundation of corporate network security. It is the responsibility of systems engineers/administrators to check if the configuration and implementation of firewalls has been completed according to a defined security policy. Accurate configuration procedure of devices is a critical mission, probably the most important factor in the security a firewall provides. Security experts commonly believe corporate firewalls to be poorly configured. Configuration quality is also interconnected with other factors such as the OS on which the firewall operates, the version of firewall software, and a access control list complexity. Insecure firewall management like firewall accesses over insecure, unencrypted, and inadequately authenticated protocols are considered as a mistake. Moreover, remote administration and misunderstanding of firewall rules can lead towards error [10][20].

Human inaccuracy while configuring and testing network devices like routers, switches and firewalls hinders effort to provide consistent, predictable end-to-end performance. Configuring the routers is most important and difficult aspect of running a large network. Configuration, of devices is time-consuming and error-prone [21].

Insufficient design and carelessness regarding the fundamentals of networking, computing, implementation and maintenance of information system can leave weakness and provides a way to attack [27]. Improper implementation of cryptographic authentication system, erroneous filtering on the routers and incorrect ACL can also leave loophole [7]. Attacker might find misconfigured system and be able to install his own root certificates, this way he/she will be capable of attempt Man-in-the-middle attack. Problem in configuration can provide a false sense of security in general circumstances [23], [24], [25].

A perfect case study of these mistakes and related vulnerabilities is the Cisco ASA 5500 firewall:

"The default configuration of Cisco ASA 5500 Series Adaptive Security Appliance (Cisco ASA) 7.0, 7.1, 7.2, 8.0, 8.1, and 8.2 allows portal traffic to access arbitrary backend servers, which might allow remote authenticated users to bypass intended access restrictions and access unauthorized web sites via a crafted URL, obfuscated with ROT13 and a certain encoding [26]."

5.1.2 Issues regarding Network Design, Installation and configuration of operating system and software used in SCADA and/or corporate network

Vulnerabilities in control system can occur because of error or misconfigurations of related application, including hardware and operating system.

Security gaps may have been inadvertently introduced within particular portion of the infrastructure. Without remedy, these gaps may represent backdoors into the control system [10]. Standard software installation, implementation or testing can possess basic flaws, if by any mean attacker gets to know these flaws, he could gain unauthorized access and control. It is important to test, patch and keep updated these devices, before and after implementation [23], [28]. "Through internal testing, Cisco has discovered that devices running Cisco IOS software may be vulnerable to DOS attack " said Jim Brady, company spokesman [29].

Knowing that 95 percent of all security breaches occur due to misconfigurations of systems or known vulnerabilities that have not been remedied? [52, p24][26, p24]

Malware; by combination of some factors like insecure or misconfigured OS and relevant software vulnerabilities, has ability to compromise information system. Software may have following vulnerabilities or deficits in its structure [19].

- It may not configured properly
- Certain functionalities turned off
- Compatibility issues with other applications
- It may also be buggy

Carelessness of the employee's part of the operation can lead to compromising the functionality of overall or some parts of the system resulting in non-availability of services. Stoppage of the service is not acceptable in any case so it is compulsory to make workflow which can effectively identify report, troubleshoot and resolve the faults that are observed [33].

For example a misconfiguration in IIS 5.0 with Index Server enabled and the Index property set in a way which allows remote attackers to list directories in the web root via a Web Distributed Authoring and Versioning (WebDAV[6]) search [34]. Such misconfigurations can provide a simple way to attempt DDOS attack [108]

5.1.3 Ports and Services Remains Open after Installation of Operating System or Application

Many platforms have a wide variety of process and services defined to operate by default. Such unneeded services could be exploited [20]. Poorly configured network equipment; by using default configurations, often leads to insecure and unnecessary open ports and exploitable network services running on hosts. Unsecured physical ports could allow unauthorized connection of thumb drives, keystroke loggers and so forth [10].

5.1.4 Wireless Link in Computer Network are Misconfigured

Wireless Technology is used for commercial and domestic purposes. It is essential to keep certain factor in view during installation and configuration [36]. Using such technology in control system environment is a risk that has to be determined by the organization [19]. Inappropriate configuration between wireless clients and access points can allow to a rogue access point to be deployed by an adversary [10].

When talking of corporate network, IT department is responsible to have updated knowledge of configuration of such devices. With the passage of time crackers have come to know that wireless is quite exposed to them because of vulnerability in configuration, encryption methods, protocols and ignorant behavior adopted or

[6] Web-based Distributed Authoring and Versioning, or WebDAV, is a set of extensions to the Hypertext Transfer Protocol (HTTP) that allows computer-users to edit and manage files collaboratively on remote World Wide Web servers

practiced by user at corporate IT level. It is necessary for the IT personals to be familiar with the tools to some extant just to neutralize the effect of cracking [19].

5.1.5 Default Setting of Devices are not Changed when Configuring

The default accounts, passwords and protection settings (system process, services and ports etc) remain unchanged during implementation. These defaults settings can be exploited by an attacker to have an unauthorized access. Unauthorized access is gained in the user's computer, network or to the equipment with eminent rights by an attacker [7]. It is possible for an individual with the available information about control system to gain unauthorized access with the use of factory-set default password. Mostly, these default passwords are never changed. Using default configurations often leads to insecure and unnecessary open ports and exploitable services and applications running on hosts [10].

For example if default setting/configuration is not changed then it is easy to exploit application program SAP R/3 using default password. SAP R/3 is transported to the user with four user accounts and these are shielded with common password [37]. Default installation of Oracle database provide many "demo" accounts with predetermined passwords [38]. Flaw in Cisco guard is indentified and reported, in which account of administrator is exposed to the attacker and he can access to it in future [39].

The default configuration of the web server in IBM Lotus Domino Server, possibly 6.0 through 8.0, enables the HTTP TRACE method, which makes it easier for remote attackers to steal cookies and authentication credentials via a cross-site tracing (XST) attack [41]

The default configuration of Sun Java System Application Server 7 and 7 2004Q2 enables the HTTP TRACE method, which makes it easier for remote attackers to steal cookies and authentication credentials via a cross-site tracing (XST) attack [42]

The default configuration of Adobe Reader and Acrobat 9.x before 9.3, and 8.x before 8.2 on Windows and Mac OS X, does not properly support the enhanced security feature, which has unspecified impact and attack vectors, related to"script injection vulnerability" [43].

The default configuration in OpenAFS[7] 1.4.x before 1.4.4 and 1.5.x before 1.5.17 supports setuid programs within the local cell, which might allow attackers to gain privileges by spoofing a response to an AFS cache manager FetchStatus request, and setting setuid and root ownership for files in the cache. [44]

The default configuration of SQL-Ledger 2.8.24 allows remote attackers to perform unspecified administrative operations by providing an arbitrary password to the admin interface. [45]

5.1.6 System Maintenance, Modification and Testing are not Completed Correctly

When system behavior is different than normal it will take some time in system maintenance. This may result in momentary, inappropriate or insecure configuration. Misconfigurations may leads to DoS and spoofing attack [7], [46]. Network equipment redundancy could be compromise during system maintenance [30].

Cutting edge operation is related to the competence of engineers, administrators, and/or operator. All these people are to maintain a system if they are not competent and they are not at ease with using procedures or equipment in an information system then it willresult in damaging or compromising the functionality of it. Installation of malware defense software without testing can cause affects of abnormal operation [19].

Lack of adequate screening or administrative procedure and awareness implies a week sense of security and incapacity to react against any threat [23]. Organizations can be left exposed to great security threat if

[7] OpenAFS is the open source release of the Andrew File System (AFS). It is a global, distributed file system used by schools and scientific laboratories around the world

implementation of Citrix is poor. Proven issues by GSS[8] testing shows that organization is vulnerable. It is vulnerable to internal system and data breach when deploying Citrix incorrectly [31]. BBC security anomaly due to an administrator error resulted in thousands of the mailing list subscribers to receive junk mails [47].

People controlling, maintaining and managing the system must be persuaded to have security. Security requirement will be eagerly adopted by the personnel if they realize the importance of it in given environment. Effectiveness of control is known when it is used. Locking computer room doors is not a good gesture. Controls must be efficient, appropriate and user friendly [48]. A tester, during the penetration testing in gas utility, mistakenly ventured into the SCADA system instead of IT Network and stopped SCADA which eventually stopped gas for around four hours. [49].

5.1.7 Access Control Policies in Computer Networks are not Implemented Correctly

Vulnerabilities are often introduced into control system environment because of improper policies or lack of policies. Poorly specified policies can result in giving user several or few privileges than required. Correct implementation of Access Control Lists (ACL), are needed to control the access of network devices. Improperly configured firewall rules and router ACLs can allow unnecessary traffic [10]. If there is no suitable internal implementation of firewalls or network access control, it can result in no separation between different segments of networks [7][50].

If the firewall policies and network management is too much complex, then it would be harder for the engineers/administrators to configure or reconfigure firewalls. Sometime Operator does not know if the system is penetrated, compromised and does not know about configuration of the firewall. This would result in difficulties regarding configuration to avoid future breaches [23].

Privileges are granted to a person, program or a device that is not required to function within the parameters and excess privileges are exploited to achieve more privilege, or else, attack the system. Unix-based setuid programs grant root access which is exploited by the attacker to gain unlimited access [51].

Viruses are less futile than the insiders, these insiders are more problematic. Attacks on any corporate networks usually come from inside than a virus. Privileged or technical users cause 87% of internal damages [91].

"An embarrassed State Department admitted today that the passport files of all three presidential candidates Sens. John McCain, Barack Obama and Hillary Clinton -- have been breached by its employees" [52], [53].

Multiple clientless SSL VPN products that run in web browsers, including Stonesoft StoneGate; Cisco ASA; SonicWALL E-Class SSL VPN and SonicWALL SSL VPN; SafeNet SecureWire Access Gateway; Juniper Networks Secure Access; Nortel CallPilot; Citrix Access Gateway; and other products, when running in configurations that do not restrict access to the same domain as the VPN, retrieve the content of remote URLs from one domain and rewrite them so they originate from the VPN's domain, which violates the same origin policy and allows remote attackers to conduct cross-site scripting attacks, read cookies that originated from other domains, access the Web VPN session to gain access to internal resources, perform key logging, and conduct other attacks [54].

5.1.8 Taking and restoration of backups are completed incorrectly

The backup of devices configuration used in control system are not maintained accurately which can cause difficulty in restoration in an event of accident thus loosing availability [10].

Data backups are the key to rapid systems recovery. But what if you reach for the backup tapes and they are not readable? What is the risk that these tapes are not written, handled, transported, and stored correctly? [121].

Your system might fail due to many causes. They may include human errors, hardware failures, transaction failures, and disasters. Human factor is one of the most common causes of system failure. For example, if a

[8] Global Secure Systems is one of the UK's largest and most experienced IT security organizations, and won 2 prestigious awards in 2008

user accidentally deletes an application group, this would trigger the removal of all data loaded into the application group [122].

Privileged programs are misused to provide illegitimate privileged functions. Description includes restoring erroneous information intentionally by using backup restoration program, misusing automated script processing facility and generating illegitimate copies of legitimate records by force [23]. Restoring information process is often misused to gather data from backup tapes.

5.1.9 Updates and Patches of Operating System and Antivirus are not Manage Properly

Operating System and control system software patches are usually not be deployed until system is not compromised or attacked by exploiting certain security vulnerabilities. There is possibility of finding newly discovered vulnerabilities in outdated Operating System and applications. Mostly the patches of such application and Operating system are implemented without in-depth testing [10].

Once a problem leaves a hole in your machine's defense, it is extremely important to patch it as soon as possible. According to the Microsoft "important and high-priority updates are critical to the security and reliability of your computer. They offer the latest protection against malicious online activities" it is recommended to update all of your programs in addition to operating system for instance Service packs, Version upgrades, Security updates and Drivers.

Several cases were witnessed where malware oriented attacks have affected critical information infrastructure directly or indirectly. Hackers, in Russia, with malicious intent got control over a gas pipe line of Gasprom by using Trojans [55].

In Jan 2003 "Slammer" worm, caused severe problems for IT systems globally and penetrated safety monitoring system at US nuclear plant for five hours [107]. US Nuclear Regulatory Commission took notice of the event and discovered that plant was infected with the MS SQL Server 2000 worm. The infection caused data overload in the site network, rendering computers unable to communicate with each other [56].

Recently US signals James Brewer involved in operating a botnet of over 10,000 computers spread all over the world, these computers also include some at CCBHS[9]. Among other things, malware infected computers frequently reboot and freeze without intimation, this affected the performance of the system as CCBHS staff witnessed delay to access the data and medical services [57], [58].

Most of the time government is unwilling to reveal the occurrence of the attack against critical infrastructure, protection and support of information system and critical infrastructure respectively has become exceptionally vital [32]. Few cases are reported in spite of these reported cases vulnerability of critical information system to attacks is known. In 2003 blackouts were witnessed in northeast US and Canada and conclusion said it was due to software failure but in depth study revealed system vulnerability to electronic attacks, through use of malware [59].

Potential security vulnerabilities have been identified with WMI Mapper for HP SIM[10]. These vulnerabilities could be exploited to allow unauthorized access to data both locally and remotely. HP provides a software patch to resolve this vulnerability [60].

Vulnerability was reported in Microsoft DNS and WINS Server. These vulnerabilities could allow a remote attacker to redirect network traffic intended for systems on the Internet to the attacker's own systems. A remote user can conduct a man-in-the-middle attack to spoof the system. This security update is rated important for all supported editions of Microsoft Windows 2000 Server, Windows Server 2003, and Windows Server 2008 [61].

[9] Cook Count Bureau of Health Service, Department of Medicine

[10] Systems Insight Manager is an IT systems management tool, used to manage computing devices, servers and storage system

A local user can obtain important privileges on the target system due to the vulnerabilities reported in the Windows Kernel. Security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008 by Microsoft [62].

5.1.10 Supporting Services or Facilities not Managed Properly

Inadequate physical protection of network equipment can cause the destruction of control system. Operation of system is quite dependent upon supporting services[11]. Interruption can be caused due to second-rated performance ability of these facilities and can damage system hardware or software. Lack of power backup to critical assets, a general loss of power will shut down the control system and could create an unsafe situation [10].

Power failure can cause loss of availability due to computer and peripheral failure which often demands for emergency response and if not completed normal operations shall be disrupted [63]. Failure of equipments also treated as major threat aligned with control and Information System [10]. Maintenance of the equipment are necessary for the system to function otherwise system will fail to perform functions. Scheduled operations can or may be mistakenly interrupted by employees. Loss magnitude depends on the services disruption duration and characteristic of the operation performed by the user. The physical characteristics of the facility housing a system may allow an intruder to get entrée both to external devices to system hardware (such as diskettes, and tapes) and to media inside system components (such as fixed disks). This can result in revealing uncovered-sensitive data. If the eavesdrop is successful and access is gained to CPU, it is possible to reboot the system and avoid logical access control. This has serious impacts and can lead to fraud, disclosure of information, introduction of Trojan horse, system and application software replacement or more [64].

5.1.11 Improper Management of Peripheral Devices

High capacity portable storage media devices are increasing and this poses enormous potential security threat to business and source of malware introduction [19]. Many employees bring Flash drives or MP3 in an organization and are plugged in USB port and OS detects it automatically. These can potentially be dangerous as these can transport data of all sorts. In this scenario there is no way to check the contents on the device and what's being transferred from and onto them when attached to corporate network. Devices can be the mean of stealing sensitive data from the organization and this can be the potential threat. The transmission of malware by the USB source is increasing [11], [65]. If sensitive data is stored on portable devices and these devices are lost or stolen, system security could be compromised. Policy, procedures, and mechanisms are required for protection [10].

Pentagon has banned the use of removable devices after unspecified virus hit on its network [66]. Commander of the U.S. Strategic Command has re-established special measures and signed an order that forbids the use of all thumb drives, flash drives, optical disks and any other removable storage devices on both the army's secret networks, effective immediately [67].

Information system is significant to security threats as it is stored in main memory of the printer, printers may stores data or information for long period and these documents can be extracted from memory by anyone who has an access on the printer

HP has intimated, hackers can steal data from PC's in which software are bundled with printers [68]. O'Conner[12] on Thursday in his presentation said "Printers are to be treated as servers and workstations". In connection to this he said printer should be managed cautiously and must be part of company's patch program, not forgotten by IT and junior staff officer controls it. O'Conner further said once he get control he is in command to map an organization internal network and this state helps him to pursue more attacks. This influence has provided him to gain access to information printed, faxed or copied from the every printer. Internal job counter can also be changed which can directly affect company bills by reducing or increasing them, if device is leased [69].

[11] Facilities like heating or cooling (AC), electricity, and telecommunication
[12] Brendan O'Connor, a security expert

5.1.12 Strong Password Policy is not Implemented Correctly and/or Password is Written down on Papers

With no password policy, systems might not have appropriate password controls, increasing possibility of unauthorized access to systems. If passwords are not changed frequently and becomes known by an unauthorized party, then that party can have unauthorized access to the network or parts of it. Such access could allow an adversary to interrupt control system operations or monitor activities. This happens if administrator is not concerned of password policies, access rights, permissions, and access control administration [70]. The observation of vulnerabilities by Test Bed NSTB[13], found password protection policies were weak [7]. To secure information system it is necessary to have password security policy. Recommendation is to have long password, words not from dictionary and should be changed often since strong password is also breakable by brute force attack [71], [72]. To avoid an incident compromising all of the accounts it is mandatory to have different passwords for each account. This will happen when user has access to numerous systems or accounts. Human imperfection, unfortunately, makes it almost impractical to coincide with all of the rules.

It is impartial to say the user is forced to write passwords somewhere if he needs to change frequently or use different passwords. It's a moral duty of user not to compromise over good passwords selection to protect confidential information; in contrast system administrator has a role to check if user acts upon it. Often system administrators do not care to demand user to change his password. Clear statement by FIPS[14] Publication [73], [74] specifies that passwords on computers operated by any agency of the U.S. Government "shall have the low practical lifetime" [75]. Finding of DeAlver [76] states when a password is selected he/she will use it for ever until and unless this is compromised.

Most of the time password is composed of few characters [76], [77] that can cause dictionary attack [78]. FIPS says password sharing among groups is not secure [79].

"Monster Database Security Breach Official Alert" announced that our database was illegally accessed and certain contact and account data were taken, including user IDs, passwords, email addresses, names and phone numbers. Monster recommended changing your password upon logging onto the site for the sake of security of your information. This is also recommended by Monster to proactively change your password yourself as an added precaution [80]. Administrator's are responsible to notify user's about the existing threats and one's that can occur in future in an organization and information sensitivity in them.

Awareness of threats and potential loss to the organization is significant for security mechanisms; without it user is likely to get tire while going through security mechanisms..

5.1.13 Log Management not Completed Properly

In computer security recording of Log[15] is obligatory and must have enough details for suitable period of time. Without proper and accurate logs, it might be impossible to determine what caused a security incident to occur. Suitable log monitoring is required to discover problems, such as misconfigurations and failures. Practice of Log analysis is advantageous to recognize security incidents, policy violation, operational problem and deceptive activity. Logging helps in auditing and forensic analysis, establishing base line, supporting internal investigation, and identifying operational trends and lasting problems. Extensive logging is practical for attempted fast and sluggish password attacks like Brute force and Dictionary Attack [5], [71], [81], [82], [83].

A fundamental problem with log management that occurs in many organizations is that no one effectively balances a limited quantity of log management resources to continuous supply of log data. Creating and storing of logs in time becomes complicated due to many factors, which includes high number of log sources, log content inconstancy as well as large volume of log data etc. This management also includes shielding

[13] National SCADA Test Bed Enhancing Control System Security in the Energy Sector
USA Department of Energy

[14] Federal Information Processing Standards

[15] Record of events happening inside an origination's system and network is known as log

confidentiality, availability and integrity of logs. To ensure security, the system and network administrator frequently checks log data and give it a full analysis, otherwise problem may arise [81], [84], [85].

5.1.14 Sensitive Information is Disclosed from Technical Staff by Means of Social Engineering

Social engineering is more or less like pretending to be an employee, calling helpdesk and inquiring employee's password [86]. Seemingly in contemporary world hacker pay more of their attention to human link rather than technical side of security for example, to gather password social engineering techniques are used [87].

Telephonic conversation can be the medium used by the attacker first to masquerade as an employee and then to convince users, administrators to give passwords, user names etc. or to convince them to execute Trojan horse programs. Human is the weakest link in an organization and policy regarding security in case of social engineering attacks should clearly state steps to avoid them. Security nowadays focuses on technical aspect of information like antivirus and firewall software. Non-technical aspects of information security are normally not taken as a serious issue in IT-security investment [88]. Many organizations have learned it the hard way that enterprise cannot be secured by security technology alone [89]. The way of overshadowing technical protection mechanism is through social engineering. "Social Engineering, once mastered, can be used to gain access on any system despite the platform or the quality of the hardware and software. It is the hardest form of attack to defend against because hardware and software alone won't stop it [90].

Social engineering is basically luring victim to commit mistake and this can be achieved by use of fake pop-ups. Victim reveals, for example, passwords in an impression to re-authenticate in order to stay connected to the network. Provided password and user name by user is sent to the Social engineer. This authentication information helps him to connect to the organization network [94]. Deception is another technique of Social Engineer accomplished by human interaction. Human ignorance and his inclination to be liked and helpful makes such attack successful. [94]. Various forms of impersonation[16] are performed like, he can play role of a repairman, fellow employee, manager, trusted third party or IT support. He masquerades[17] to gain unauthorized trust[93]. Two men were arrested who committed a crime of extracting billions of Yens from Softbank Corp. This was accomplished by obtaining password to the bank database from an ex- bank worker, Data was copied and this incident took place [95]. Motive was clear to escape with billions from bank. Former worker provide them with the password that was used to access the database of the bank.

[16] Someone who imitates or copies the behavior or actions of another
[17] Pretend to be someone or something that you are not

6 SURVEY RESULT AND ANALYSIS

This chapter presents the identified Causes and Mistakes, their probabilities as obtained from the literature review and interview methodology discussed earlier, the relationships between these causes and mistakes and last but not the least, the Bayesian Network representing all of the aforementioned.

The probabilities of mistakes[18] and their causes[19] were put in a Bayesian Network and simulated in GeNIe[20]. From this simulation we were able to obtain the probability of occurrence of each of the mistakes. By doing so, we were able to show the impact of each of the causes on the mistakes as a numerical measure. Furthermore, the impact of each of these causes was analyzed individually. This gave us an individual measure of the impact of each of the causes.

[18] List of mistakes has been prepared during literature study
[19] List of causes based on mistakes has been taken from experts
[20] GeNIe is a development environment for building graphical decision-theoretic models

6.1 Bayesian Model of Identified Causes and Mistakes

The following model was reached after the literature studies and the three phase interviews. It represents the relationship of mistakes and causes. It was achieved after adding the probabilities given by experts in variable causes and mistakes nodes in Bayesian Network. The general case as shown in Figure 8 below, represents the identified mistakes made in a project. The method of getting the probability of causes from experts has been explained in section 5.3.

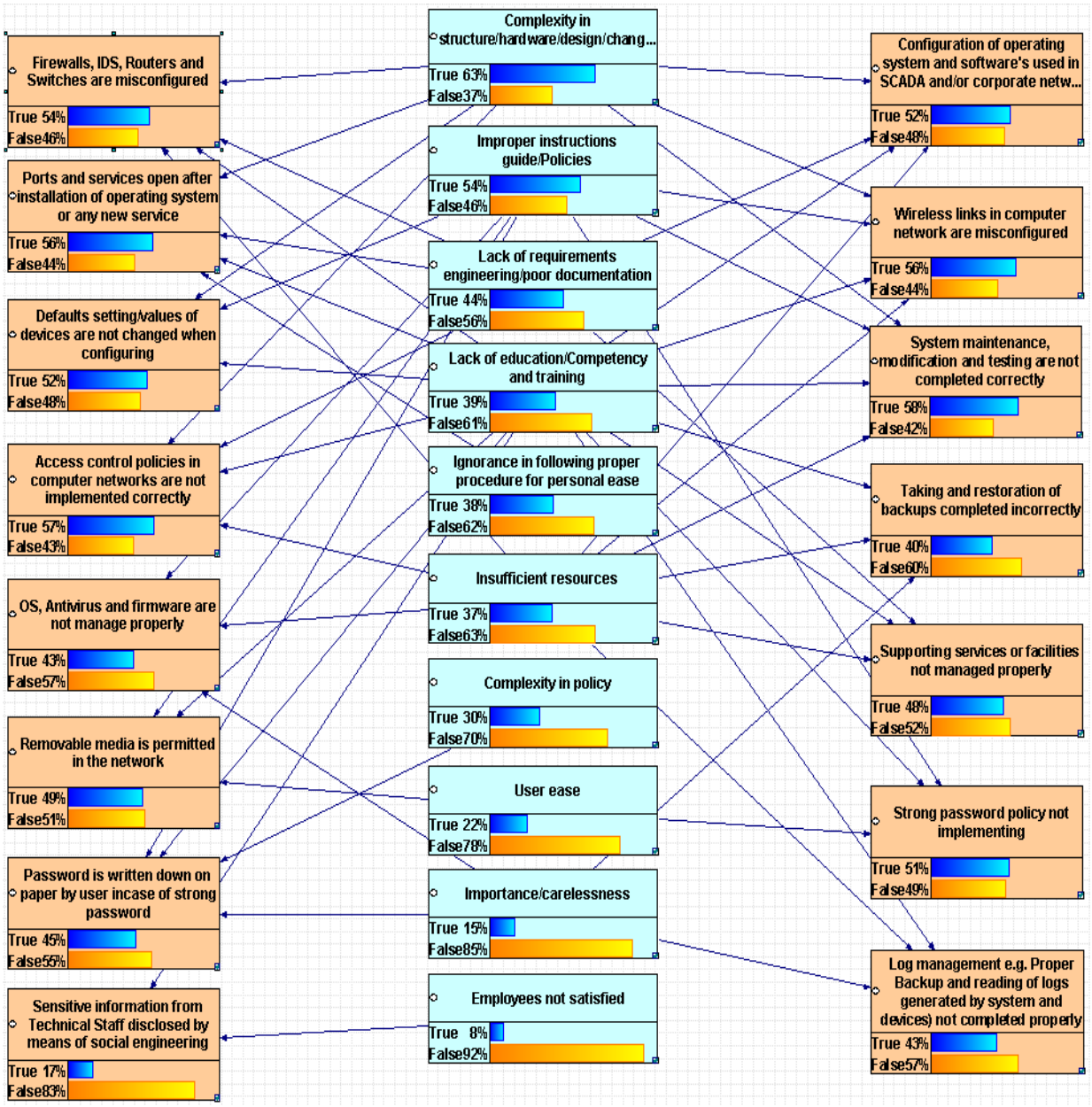

Figure 8 - Model illustrates probability distribution.

The model shown in Figure 8 above shows the calculated probabilities. The nodes in the middle column represent the causes while the nodes at the left and right denote the mistakes. The arrows from cause nodes to

the mistake nodes show the influence from causes to mistakes. The blue bars in the nodes show that the condition exists by the expressed percentage. Similarly, the yellow bars show the probability of the condition when it does not exist. The following sections discuss the major causes and mistakes identified by arriving at the model above. We decided that any mistakes having probability greater than 50% had a greater overall impact. So we will try to identify these major mistakes and their causes which are correlated and then try to reach a conclusion.

6.1.1 Identified Causes

The top cause of mistakes was identified to be 'Complexity in structure/hardware/design/changes in the configuration' (63%) while the cause 'Employees not satisfied' had the least impact (8%). Among all the causes, the most occurring ones seemed to have the most impact too. Among these were causes 1 till 4 as shown in the table below.

Table 5 - Identified causes of mistakes in a Project

Ranking	Causes	Probabilities
1	Complexity in structure/hardware/design/changes in the configuration	63%
2	Improper instructions guide/ Policies	54%
3	Lack of requirements engineering/poor documentation	44%
4	Lack of education/Competency and training	39%
5	Ignorance in following proper procedure for personal ease	38%
6	Insufficient resources	37%
7	Complexity in policy	30%
8	User ease	22%
9	Importance/carelessness	15%
10	Employees not satisfied	8%

6.1.2 Identified Mistakes

Table 6 below presents the outcome of variables on the basis of collected information. We can say that the probability of 'incorrect system maintenance, modification and testing' is the highest, i.e., 58%. The next is the 'improper access control policies implementation' at 57%. 'Ports and services remains open after installation' and 'wireless network misconfigurations' are third at 56%. Then its 'Firewalls, IDS, Routers and Switches misconfiguration' (54%), 'improper Installation and configuration of operating system and software' (52%), 'possibility of deliver system with default settings' (52%) and 'possibility of improper implementation of password policy' (51%).
These were the eight most occurring mistakes out of a total of 15 identified mistakes having a probability greater than 50%. We focused on these mistakes for the analysis as they were the most affecting and most occurring.

Table 6 - Identified mistakes that are made in a Project

Ranking	Mistakes	Probabilities
1	System maintenance, modification and testing are not completed correctly	58%
2	Access control policies in computer networks are not implemented correctly	57%
3	Unneeded Ports and services remain open after installation of operating system or application??	56%
4	Wireless links in computer network are misconfigured	56%
5	Firewalls, IDS, Routers and Switches are misconfigured	54%
6	Installation and configuration of operating system and software used in SCADA and/or corporate network are not completed correctly	52%
7	Default setting/values of devices are not changed when configuring	52%
8	Strong password policy not implemented e.g. minimum password length, use of alpha-numeric and special characters	51%
9	Peripheral Devices are not managed properly	49%
10	Supporting services or facilities not managed properly	48%
11	Password is written down on paper by user incase of strong password	45%
12	Updates and Patches of OS, Antivirus and firmware are not manage properly	43%
13	Log management e.g. Proper Backup and reading of logs generated by system and devices) are not completed properly	43%
14	Taking and restoration of backups are completed incorrectly	40%
15	Sensitive information from Technical Staff disclosed by means of social engineering	17%

6.1.3 Influence of Causes on Mistakes

The top eight mistakes having probabilities greater than 50% as identified earlier were analyzed. It was found that the main causes pointed out in the previous sections had a major contribution towards the occurrence these mistakes. Of all the four main causes, each had a major impact on the eight critical mistakes. Upon further analysis we found that these four causes largely influenced almost all the mistakes. The rest of the causes had lesser or negligible impact.

To validate the above statement, we set evidence on these four major causes (applied or removed causes in the model) and observed the outcome as shown in the Figure 9 and Figure 10 below.

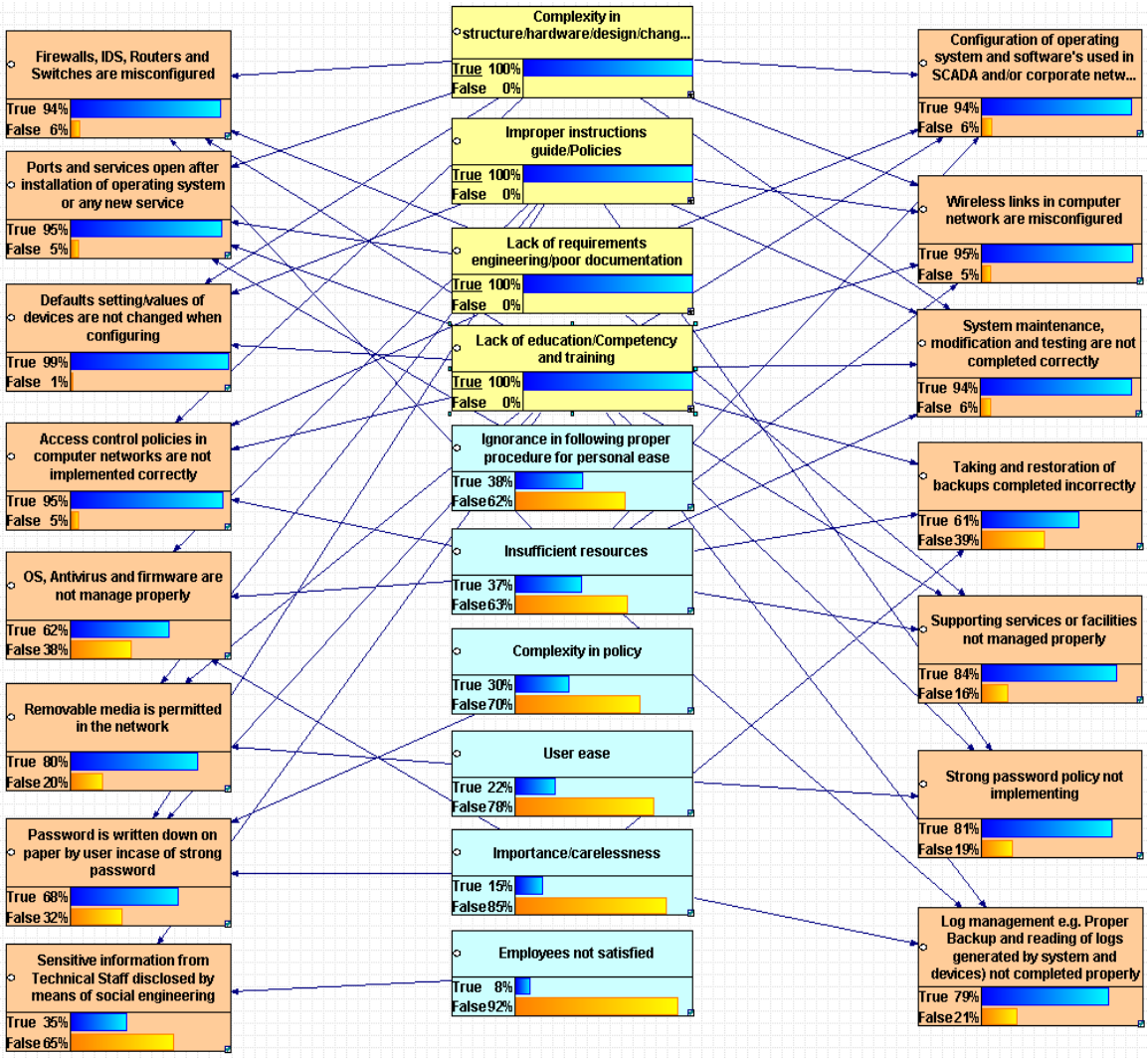

Figure 9 - Influence on mistakes when main causes are present

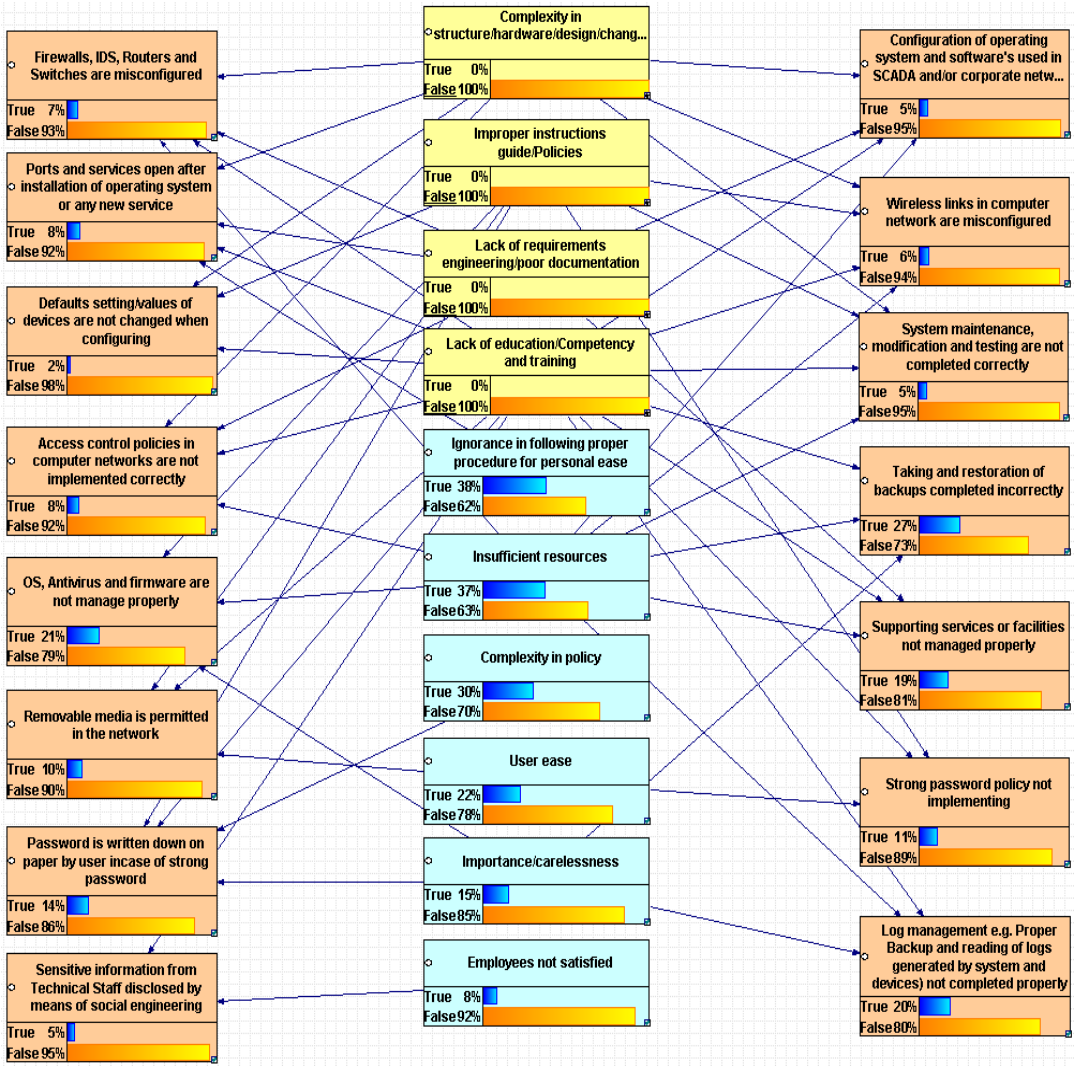

Figure 10 - Influence on mistakes when main causes are absent

6.1.4 Validation of Results

We confirmed these results by simulating the model for all the causes step by step for both absence and presence conditions. The result of this exercise is presented in Tables 7 and 8 below. These show and also justify our argument that the probability of mistakes increases or decreases as we start to include or exclude the causes. The tables give a clear picture how setting evidence for one or more causes impacts the probability of mistakes. It can be noted that after the evidence is set for the first four causes, there is little or no change in the probabilities. Hence, we can say that these causes are more critical and we shall try to focus them when suggesting mitigation strategy.

6.1.5 Validate Effect of Presence of Causes

The model was simulated to observe the probability of mistakes after each cause from A to J as listed below was introduced. We simulated the model with 100% presence of the variable cause nodes one by one to compare the probability of mistakes as we introduce each cause.

- A = Complexity in structure/hardware/design/changes in the configuration
- B = Improper instructions guide/ Policies
- C = Lack of requirements engineering/poor documentation
- D = Lack of education/Competency and training
- E = Ignorance in following proper procedure for personal ease
- F = Insufficient resources
- G = Complexity in policy
- H = User ease
- I = Importance/carelessness
- J = Employees not satisfied

Table 7 below shows the result of this experiment where the columns in red represent the drastic change in probabilities of mistakes as each of the major causes is added. The columns in yellow represent the same for the rest of the causes. It is obvious that they have a negligible effect on the probabilities of mistakes.

Table 7 - Step by Step inclusion of causes

Mistakes	A = 100% True	A to B = 100% True	A to C= 100% True	A to D = 100% True	A to E = 100% True	A to F = 100% True	A to G = 100% True	A to H = 100% True	A to I = 100% True	A to J = 100% True
Firewalls, IDS, Routers and Switches are misconfigured	61%	61%	78%	94%	94%	98%	98%	98%	98%	98%
Installation and configuration of operating system and software used in SCADA and/or corporate network are not completed correctly	61%	61%	78%	94%	94%	99%	99%	99%	99%	99%
Unneeded Ports and services remain open after installation of operating system or application??	65%	65%	87%	95%	100%	100%	100%	100%	100%	100%
Wireless links in computer network are misconfigured	64%	80%	80%	95%	95%	99%	99%	99%	99%	99%
Default setting/values of devices are not changed when configuring	58%	78%	78%	99%	99%	99%	99%	99%	99%	99%
System maintenance, modification and testing are not completed correctly	65%	81%	81%	94%	94%	100%	100%	100%	100%	100%
Access control policies in computer networks are not implemented correctly	66%	66%	81%	95%	95%	99%	99%	99%	99%	99%
Taking and restoration of backups are completed incorrectly	40%	40%	40%	61%	61%	71%	71%	71%	96%	96%
Updates and Patches of OS, Antivirus and firmware are not manage properly	43%	62%	62%	62%	62%	75%	75%	75%	98%	98%
Supporting services or facilities not managed properly	48%	48%	70%	84%	84%	95%	95%	95%	95%	95%
Peripheral Devices are not managed properly	49%	74%	74%	80%	80%	80%	80%	98%	98%	98%
Strong password policy not implemented e.g. minimum password length, use of alpha-	51%	74%	74%	81%	81%	81%	81%	97%	97%	97%

numeric and special characters										
Password is written down on paper by user incase of strong password	45%	60%	60%	68%	68%	68%	83%	83%	100%	100%
Log management e.g. Proper Backup and reading of logs generated by system and devices) not completed properly	43%	43%	43%	79%	79%	83%	83%	83%	99%	99%
Sensitive information from Technical Staff disclosed by means of social engineering	17%	17%	17%	35%	35%	35%	35%	35%	35%	82%

6.1.6 Validate Effect of Absesnce of Causes

Alternatively, we removed variable cause nodes similar to how it was done for inclusion in the previous section. This again proved the major impact of the four main causes (red columns in the table) identified earlier. The Table 8 below shows the outcome of probability of mistakes after step by step exclusion of A to J cause nodes.

- A = Complexity in structure/hardware/design/changes in the configuration
- B = Improper instructions guide/ Policies
- C = Lack of requirements engineering/poor documentation
- D = Lack of education/Competency and training
- E = Ignorance in following proper procedure for personal ease
- F = Insufficient resources
- G = Complexity in policy
- H = User ease
- I = Importance/carelessness
- J = Employees not satisfied

Table 8 - Step by Step exclusion of causes

Mistakes	A = 100% False	A to B = 100% False	A to C= 100% False	A to D = 100% False	A to E = 100% False	A to F= 100% False	A to G = 100% False	A to H = 100% False	A to I = 100% False	A to J= 100% False
Firewalls, IDS, Routers and Switches are misconfigured	42%	42%	26%	7%	7%	1%	1%	1%	1%	1%
Installation and configuration of operating system and software used in SCADA and/or corporate network are not completed correctly	37%	37%	20%	5%	5%	1%	1%	11%	1%	1%
Unneeded Ports and services remain open after installation of operating system or application??	41%	41%	20%	8%	3%	3%	3%	3%	3%	3%
Wireless links in computer network are misconfigured	43%	16%	16%	6%	6%	1%	1%	1%	1%	1%
Default setting/values of devices are not changed when configuring	42%	48%	18%	2%	2%	2%	2%	2%	2%	2%
System maintenance, modification and testing are not completed correctly	46%	23%	23%	5%	5%	1%	1%	1%	1%	1%
Access control policies in computer networks are not implemented correctly	42%	42%	25%	8%	8%	1%	1%	1%	1%	1%
Taking and restoration of backups are completed incorrectly	40%	40%	40%	27%	27%	10%	10%	10%	3%	3%
Updates and Patches of OS, Antivirus and firmware are not manage properly	43%	21%	21%	21%	21%	10%	10%	10%	4%	4%
Supporting services or facilities not managed properly	48%	48%	30%	19%	19%	4%	4%	4%	4%	4%

Peripheral Devices are not managed properly	49%	20%	20%	10%	10%	10%	10%	3%	3%	3%
Strong password policy not implemented e.g. minimum password length, use of alpha-numeric and special characters	51%	24%	24%	11%	11%	11%	11%	5%	5%	5%
Password is written down on paper by user incase of strong password	45%	27%	27%	14%	14%	14%	8%	8%	4%	4%
Log management e.g. Proper Backup and reading of logs generated by system and devices) are not completed properly	43%	43%	43%	20%	20%	6%	6%	6%	1%	1%
Sensitive information from Technical Staff disclosed by means of social engineering	17%	17%	17%	5%	5%	5%	5%	5%	5%	2%

6.1.7 Strength of Influence

As a second level of validation, we verified our validation by calculating the strength of influence of cause nodes on mistake nodes. The influence of all the cause nodes on mistake nodes was averaged based on the values in the general Bayesian model presented in section 7.1.

The output of this strength of influence calculation identified the causes which had the most influence on the mistakes. As shown in Figure 11 below, average influences between nodes are shown as arcs between them. These arcs vary in thickness proportional to the average value.

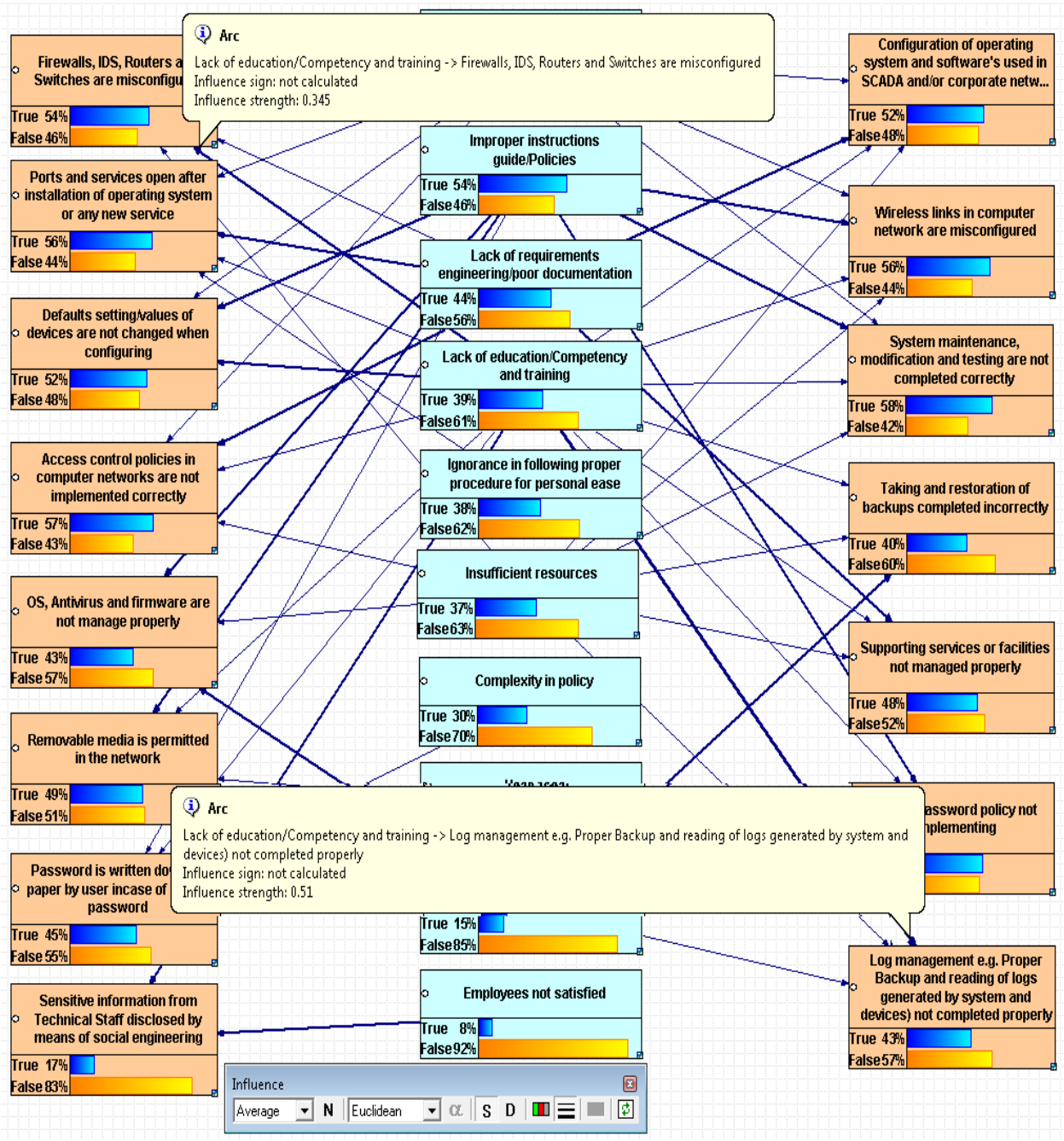

Figure 11 - Strength of influence of causes on mistakes

The Table 9 below shows the strength of influence in percentage. These values have been taken from the model generated as shown in Figure 11 above. It is an important result as the five most strongly influencing causes contain three of the causes identified in our previous analysis. This serves as a verification and validation of our initial results.

Table 9 - Shows Strength of Influence

Causes	Influenced Mistakes	Percentage of Impact
Improper instructions guide/ Policies	Default setting/values of devices are not changed when configuring.	42%
	OS, Antivirus and firmware are not managed properly.	35%
	Removable media is permitted in the network.	48%
	Wireless links in computer network are misconfigured.	40%
	System maintenance, modification and testing are not completed correctly.	36%
	Strong password policy not implementing.	47%
Lack of requirements engineering/poor documentation	Ports and services open after installation of operating system or any new service.	41%
	Access control policies in computer networks are not implemented correctly.	30%
	Sensitive information from Technical Staff disclosed by means of social engineering.	37%
	Configuration of operating system and software used in SCADA and/or corporate network are not completed correctly.	32%
	Supporting services or facilities not managed properly.	38%
Lack of education/Competency and training	Firewalls, IDS, Routers and Switches are misconfigured.	34%
	Default setting/values of devices are not changed when configuring.	35%
	Log management e.g. Proper Backup and reading of logs generated by system and devices) are not completed properly.	51%
Importance/carelessness	OS, Antivirus and firmware are not managed properly.	31%
	Taking and restoration of backups are completed incorrectly.	34%
Employees not satisfied	Sensitive information from Technical Staff disclosed by means of social engineering.	42%

From the results and analyses drawn from the results presented, we can now say that the causes that had the most impact in our case are as follows:

1. Complexity in structure/hardware/design/changes in the configuration
2. Improper instructions guide/ Policies
3. Lack of requirements engineering/poor documentation
4. Lack of education/Competency and training
5. Importance/carelessness
6. Employees are not satisfied

We have now identified the main causes of mistakes and shortlisted them to a total of six critical causes which we shall focus for now to suggest our mitigation strategy.

7 MITIGATIONS

This chapter discusses the suggested mitigation strategies for the identified main causes and mistakes.

The following table presents the causes identified in the previous sections. Against each of these causes are listed the mistakes along with their mitigation strategies. It can be seen from the table that all of these causes affect more than one mistake. Hence, if we reduce one cause, it will automatically reduce the probability of more than one mistake and the threats associated with them.

Table 10 - Main causes and their mistakes with their mitigation strategies

<table>
<tr><td colspan="2">Cause: Complexity in structure/hardware/design/changes in the configuration</td></tr>
<tr><td>Influenced Mistakes</td><td>Mitigation</td></tr>
<tr><td>Firewalls, IDS, Routers and Switches are misconfigured.</td><td rowspan="7">Reduce the complexity involved in configuration of Firewalls, Routers and Switched by improving the documentation.

Training and awareness about vulnerabilities in the system and network.

Processes, guidelines and checklists to streamline the method of configuration.

Well defined test methods which are easy to execute.</td></tr>
<tr><td>Configuration of operating system and software used in SCADA and/or corporate network are not completed correctly.</td></tr>
<tr><td>Ports and services open after installation of operating system or any new service.</td></tr>
<tr><td>Wireless links in computer network are misconfigured.</td></tr>
<tr><td>Default setting/values of devices are not changed when configuring.</td></tr>
<tr><td>System maintenance, modification and testing are not completed correctly.</td></tr>
<tr><td>Access control policies in computer networks are not implemented correctly.</td></tr>
<tr><td colspan="2">Cause: Improper instructions guide/ Policies</td></tr>
<tr><td>Default setting/values of devices are not changed when configuring.</td><td rowspan="6">Creation and implementation of policies for Operating System installation/configuration.

Policies and guidelines for accessibility of network resources sharing, strong password and for the use of peripherals.

Implement principal of least privilege as default policy to avoid vulnerabilities in the future.

The policies for administrators describing the portion of modifying the systems design, hardware, software, firmware's and OS must be enforced. This provides adequate guarantee that the system is well protected against improper modification before, during and after</td></tr>
<tr><td>OS, Antivirus and firmware are not managed properly.</td></tr>
<tr><td>Removable media is permitted in the network.</td></tr>
<tr><td>Wireless links in computer network are misconfigured.</td></tr>
<tr><td>System maintenance, modification and testing are not completed correctly.</td></tr>
<tr><td>Strong password policy not implementing.</td></tr>
</table>

	implementation. Suitable management and implementation of ACL are necessary to reduce this factor.
Cause: Lack of requirements engineering/poor documentation	
Firewalls, IDS, Routers and Switches are misconfigured.	Improve documentation for instance, instruction manuals, guidelines, and checklists. Adopt a better requirement gathering methodology which maintains logs of changes during the process and ensures distribution of requirements to the involved personnel. Availability of updated user manuals and sufficient requirement engineering for installation and configuration.
Ports and services open after installation of operating system or any new service.	
Access control policies in computer networks are not implemented correctly.	
Configuration of operating system and software used in SCADA and/or corporate network are not completed correctly.	
Supporting services or facilities not managed properly.	
Cause: Lack of education/Competency and training	
Firewalls, IDS, Routers and Switches are misconfigured.	Skilled staff to handle these issues and this can be achieved by education. Training and awareness about vulnerabilities in the system and network. Constant improvement: While initial training is good, it is important to keep updated by learning about new possibilities in the security domain. Knowledge of policies, procedures and if necessary to follow security training in order to perform their roles with responsibility. Privileged users have to be well trained to exercise their privileges properly. Hiring of trained and educated staff.
Ports and services open after installation of operating system or any new service.	
Default setting/values of devices are not changed when configuring.	
Access control policies in computer networks are not implemented correctly.	
Removeable media is permitted in the network	
Strong password policy not implementing.	
Sensitive information from Technical Staff disclosed by means of social engineering.	
Configuration of operating system and software used in SCADA and/or corporate network are not completed correctly.	
Wireless links in computer network are misconfigured.	
System maintenance, modification and testing are not completed correctly.	
Taking and restoration of backups are completed incorrectly.	

Supporting services or facilities are not managed properly	
Log management e.g. Proper Backup and reading of logs generated by system and devices) are not completed properly.	
Cause: Importance/carelessness	
OS, Antivirus and firmware are not managed properly.	Secure wireless hubs and encryption techniques. Awareness and training along with motivation towards following procedures. On time deployment of updates, the surety of all hosts and network equipment is updated with the latest tested and verified security patches available. Suitable configuration, maintenance, and modification policy implementation, high-quality patch management. Accurate taking and resorting of backups, supporting services management and log management. Accountability of individuals responsible for performing, testing, storing, and restoring backups. Recent local backups should be available for immediate use and secure backups must be available to recover from a massive security incident. A well defined backup method should be used to ensure that backups are strictly produced, securely stored, and appropriately accessible for restoration.
Password is written down on the papers by users in case of strong password policy	
Taking and restoration of backups are completed incorrectly.	
Log management e.g. Proper Backup and reading of logs generated by system and devices) are not completed properly.	
Cause: Employees not satisfied	
Sensitive information from Technical Staff disclosed by means of social engineering.	Policies, training and awareness of employees together with better education.

8 CONCLUSION

SCADA systems have been used for decades in the utilities industry with great success. Now more than ever, it is important that our critical infrastructure such as power grids, water processing systems, and public switched networks, be monitored and protected. The aim of this research project was to investigate the main causes for security being compromised in automation control systems. Also, to find out which of these causes had the most effect in terms of mistakes and how to mitigate them?

Using the literature study we gathered mistakes and then used surveys to identify some causes which lead to these mistakes which in turn created vulnerabilities in the systems. These causes were put in a Bayesian Network to find their influences on the mistakes which lead to the selection of six main causes that largely affected most of the mistakes that occurred. The resulting model was used to analyze different cases and also to validate our initial analysis of the collected causes and mistakes.

The research questions that we tried to answer in this study are discussed below:

What are the main mistakes for security being compromised in automation control systems?

Based on the extensive literature study, we identified common mistakes that are committed during projects. During the analysis, we shortlisted eight of fifteen main mistakes that had a major impact. These are listed below:

1. System maintenance, modification and testing are not completed correctly
2. Access control policies in computer networks are not implemented correctly
3. Unneeded Ports and services remain open after installation of operating system or application??
4. Wireless links in computer network are misconfigured
5. Firewalls, IDS, Routers and Switches are misconfigured
6. Installation and configuration of operating system and software used in SCADA and/or corporate network are not completed correctly
7. Default setting/values of devices are not changed when configuring
8. Strong password policy not implemented e.g. minimum password length, use of alpha-numeric and special characters

What are the main causes of mistakes?

Based on the outcome of our analysis, we identified several causes and reduced them into categories to cover all possible causes of mistakes. The analysis was supported by simulating a Bayesian model of the causes and mistakes. By calculating the influence of causes on mistakes, we were able to pinpoint the major causes as listed below:

1. Complexity in structure/hardware/design/changes in the configuration
2. Improper instructions guide/ Policies
3. Lack of requirements engineering/poor documentation
4. Lack of education/Competency and training
5. Importance/carelessness
6. Employees are not satisfied

These influencing causes of human mistakes were found to have significantly high occurrence probabilities. At the same time, these figures correspond to real life instances of mistakes. As these were the causes that had the most effect on occurrence of mistakes, the same were focused to suggest mitigation strategies.

What should be done to mitigate these causes?

The mitigation strategies discussed in detail in chapter 8 were based on the main causes and mistakes identified. The strategies were based on the vulnerabilities and threats posed by these mistakes and essentially their causes.

We suggested mitigation strategies to eliminate these mistakes. These strategies were suggested according to the recent trends and state-of-the-art technology in use these days. The mitigation steps included awareness and training of personnel together with proper policies, documentation and processes.

To sum up, realizing training existing personnel and hiring skilled personnel may bring changes to the way in which they access, install, configure, modify, test, operate, control and manage server machines, workstations and devices used in control systems. Organizations need to improve the security of their systems by focusing on the aforementioned causes. With the suggested mitigations strategies, security of automation control systems can be greatly improved.

We can say that using the approach adopted in this study, vulnerabilities can be identified and security of large network systems, especially SCADA systems can be ensured and improved over time.

9 REFERENCE

[1] JOSE J GONZALEZ, AGATA SAWICKA
A Framework for Human Factors in Information Security
© WSEAS – Presented at the 2002 WSEAS Int. Conf. on Information Security,
Rio de Janeiro, 2002 [Online] http://ikt.hia.no/josejg/

[2] Kizza, Joseph Migga
Computer Network Security / Joseph Migga Kizza
Department of Computer Science
314B EMCS, University of Tennessee-Chattanooga 615 McCallie Avenue

[3] SearchNetworking.com [Online]
http://searchnetworking.techtarget.com/news/article/0,289142,sid7_gci963204,00.html

[4] SAN Institute InfoSec Reading Room
The Weakest Link: The Human Factor Lessons Learned from the German
WWII Enigma Cryptosystem

[5] The Information Warfare Site (IWS) Critical Infrastructure Protection (CIP),
Understanding SCADA System Vulnerabilities, 2001, pp 1, [online],
http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf

[6] National Research Council (U.S.), Computer Science and Telecommunications
Board Staff (CB). *Cybersecurity Today and Tomorrow: Pay Now or Pay Later*.
Washington, DC, USA: National Academies Press, 2002

[7] Raymond K.Fink, David F. Spencer, Rita A. Wells. Lessons Learned from Cyber Security Assessment of
SCADA and Energy Management Systems, National SCADA Test Bed (NSTB), 2006, [online],
http://www.inl.gov/scada/publications/d/nstb_lessons_learned_from_cyber_security_
assessments.pdf

[9] Chee-Wooi Ten, Student and Chen-Ching Liu
Cybersecurity for Electric Power Control and Automation Systems

[10] Keith Stouffer, Joe Falco, Karen Scarfone
Guide to Industrial Control Systems (ICS) Security
Recommendations of the National Institute of Standards and Technology
Special Publication 800-82

.

[11] Richards, Guy. Hacker v Slackers, The IET Knowledge Network, 2008, [online],
http://kn.theiet.org/magazine/issues/0819/hackers-slackers-0819.cfm

[12] M2 PRESSWIRE-30 May 2003-SoftwareByBay [Online]
http://findarticles.com/p/articles/mi_hb5243/is_200305/ai_n19624221?tag=rel.res1

[15] Smith J.N, Merna T, Jobling P. Managing Risk in Construction Projects,
Blackwell Publishing, 2006.

[16] David Heckerman, Technical Report MSR-TR-95-06 A Tutorial on Learning With Bayesian Networks
March 1995 (Revised November 1996)

[17] Marek J. Druzdzel, Linda C. van der Gaag
Building Probabilistic Networks: Where Do the Numbers Come From? — a Guide to the
Literature

[18] May Robin Permann, Kenneth Rohde
Cyber Assessment Methods for SCADA Security
Information & Communications Systems, Cyber Security Technologies
Idaho National Laboratory

[19] Keith Stouffer, Joe Falco, Karen Scarfone. Guide to Industrial Control Systems (ICS) Security. Special Publication 800-82 SECOND PUBLIC DRAFT

[20] Avishai Wool, Tel Aviv University
A Quantitative Study of Firewall Configuration Errors

[21] Don Caldwell, Anna Gilbert, Joel Gottlieb, Albert Greenberg, Gisli Hjalmtysson, and Jennifer Rexford. The Cutting EDGE of IP Router Configuration

[22] James Michael Stewart Ed Tittlel, Mike Chapple
CISSP Certified Information Systems Security Professional Study Guide 3rd Edition

[23] Anton, Philip S. Finding and Fixing Vulnerabilities in Information Systems : The Vulnerability Assessment and Mitigation Methodology.
Santa Monica, CA, USA: Rand Corporation, The, 2003. p 25.

[24] Burkholder, Peter. "SSH and SSL for SysAdmins," 24 January 2002.[Online]
http://www.pburkholder.com/sysadmin/UW_SSL_talk/index.html

[25] Rasool Azari, University of Redlands, USA
Current Security Management & Ethical Issues of Information Technology

[26] NIST – National Institute of Standard and Technology .National Vulnerability Database, Vulnerability Summary for CVE-2009-4455. Release date 12/29/2009
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-4455

[27] Salah Alabady, Design and Implementation of a Network Security Model for Cooperative Network
Computer Engineering Department, University of Mosul, Iraq
International Arab Journal of e-Technology, Vol. 1, No. 2, June 2009,

[28] Center for the Protection of National Infrastructure (CPNI), Electronic attacks, [online],
http://www.cpni.gov.uk/MethodsOfAttack/electronic.aspx

[29] Cisco warns of network flaw, Published: 17 Jul 2003 10:31 BST [Online]
http://news.zdnet.co.uk/itmanagement/0,1000000308,2137710,00.htm

[30] Skendzic V, Guzman A. Enhancing power system automation through the use of real-time Ethernet, Power Systems Conference: Advanced Metering, Protection, Control, Communication and Distributed Recourses, 2006, pp. 480-495. [Online] www.selinc.com/techpprs/6188_EnhancingPower_20041114.pdf

[31] Security Park - The leading online News portal for Security professionals [Online]
http://www.securitypark.co.uk/security_article.asp?ArticleID=261919

[32] A recent OECD Report: The Development of Policies to Protect the Critical Information
Infrastructure highlights this point. See DSTI/ICCP/REG(2007)20/FINAL.

[33] NETWORK OPERATIONS CENTER DESIGN AND IMPLEMENTATION
2005 COMPUTERWORLD HONORS CASE STUDY

[34] NIST – National Institute of Standard and Technology .National Vulnerability Database, Vulnerability Summary for CVE-2000-0951. Release Date 12/19/2000 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-0951

[36] Computer Crime Research Center [Online] http://www.crime-research.org/articles/wireless-security-some-measures/

[37] "SAP R/3 Default Password Vulnerability", Beyond Security Ltd., August 26, 2002. [Online] http://www.securiteam.com/securitynews/5YP0N1P80O.html

[38] SecurityFocus Microsoft Newsletter #71. [Online]

[39] Secunia [Online] http://secunia.com/advisories/13484/

[41] NIST – National Institute of Standard and Technology .National Vulnerability Database, Vulnerability Summary for CVE-2008-7253. Release Date 01/25/2010 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7253

[42] NIST – National Institute of Standard and Technology .National Vulnerability Database, Vulnerability Summary for CVE-2010-0386. Release Date 01/25/2010 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386

[43] NIST – National Institute of Standard and Technology .National Vulnerability Database, Vulnerability Summary for CVE-2009-3956. Release Date 01/13/2010. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3956

[44] NIST – National Institute of Standard and Technology .National Vulnerability Database, Vulnerability Summary for CVE-2007-1507. Release Date 03/20/2007 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-1507

[45] NIST – National Institute of Standard and Technology .National Vulnerability Database, Vulnerability Summary for CVE-2009-4402. Release Date 12/23/2009 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-4402

[46] Cisco. "Strategies to Protect Against Distributed Denial of Service Attacks". 17 February 2000

[47] Incorporating IT Week [Online] http://www.computing.co.uk/tags/security

[48] Charles P.Pfleeger, Shari Lawrence Pfleeger Computing in Security, 3rd Edition, Prentice Hall,2003

[49] Duggan P. David. Penetration Testing of Industrial Control Systems, SANDIA Report, 2005, [online], http://www.sandia.gov/scada/documents/sand_2005_2846p.pdf

[50] Anton, Philip S. Finding and Fixing Vulnerabilities in Information Systems : The Vulnerability Assessment and Mitigation Methodology.

[51] Cynthia Phillips, Laura Painton Swiler, Timothy Gaylor, Patricia Leary, Fran Rupley, Richard Isler, and Eli Dart A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses;A Cause and Effect Model; and Some Analysis Based on That Model

[52] Chris Bauserman, Tim Hahn Privileged user management, monitoring and control.May 18 - 22, 2008|Orlando, Florida

[53] ABC News, Passport Security Breach on McCain, Clinton & Obama.KIRIT RADIA. WASHINGTON, March 21, 2008.

[54] NIST – National Institute of Standard and Technology .National Vulnerability Database, Vulnerability Summary for CVE-2009-2631. Release Date 12/04/2009 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2631

[55] Bernadette H. Schell and Clemens Martin, Cybercrime. Denning, Dorothy (2000).

[56] UNITED STATES NUCLEAR REGULATORY COMMISSION. OFFICE OF NUCLEAR REACTOR REGULATION. WASHINGTON, DC 20555-0001, August 29, 2003

[57] Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL Maalcious Software (Malware) A Security Threat to the Internet Economy Seoul, Korea, 17-18 June 2008

[58] COMMISSION OF THE EUROPEAN COMMUNITIES. Brussels, 30.3.2009, SEC(2009) 399 COMMISSION STAFF WORKING DOCUMENT, Accompanying document to the COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE UROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience" SUMMARY OF THE IMPACT ASSESSMENT. COM(2009) 149, SEC(2009) 399

[59] A recent OECD Report: The Development of Policies to Protect the Critical Information Infrastructure highlights this point. See DSTI/ICCP/REG(2007)20/FINAL.

[60] Microsoft Security Bulletin MS09-006, Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690) March 10, 2009

[61] Microsoft Security Bulletin MS09-008, Vulnerabilities in DNS and WINS Server Could Allow Spoofing (962238) March 10, 2009 | Updated: May 12, 2009

[62] CVE-2009-0712, CVE-2009-0713 http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01655638

[63] Fred Cohen, Cynthia Phillips, Laura Painton Swiler, Timothy Gaylor, Patricia Leary, Fran Rupley, Richard Isler, and Eli Dart. Sandia National Laboratories, September, 1998 A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses; A Cause and Effect Model; and Some Analysis Based on That Model

[64] Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook.[Online] http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter15.html#103

[65] Security threat report: 2009, By SOPHOS [Online] www.sophos.com

[66] Richard Adhikari, November 21, 2008: [Online] www.internetnews.com

[67] SOFTPEDIA, Lucian Constantin, Web News Editor: 21st of November 2008, 10:56 GMT

[68] Antony Savvas, Posted: 11:35 06 Apr 2006 Computer Weekly.com [Online] www.computerweekly.com

[69] August 7, 2006. Printer Security. At BlackHat Talk [Online]

http://news.cnet.com/Printers-a-weak-link-in-network-security/2100-1002_3-6102367.html

[70] Jacobs, Josh. SSCP Study Guide & DVD Training System. Rockland, MA, USA: Syngress Publishing, 2003.

[71] Stewart, J. M. CISSP Professional : Certified Information Systems Security Professional Study Guide. Alameda, CA, USA: Sybex, Incorporated, 2005

[72] http://www.tech-faq.com/brute-force-attack.shtml

[73] Anne Adam and Martina Angela Sasse, "Users are not the enemy,"CommunicafionrofrheACM42:12, December 1999, pp. 4046.

[74] Jason Hiner, "Change your company's culture to combat Social Engineering attacks" http://techrepublic.com.com/5100-6264-1047991.html, 2005-01-30

[75] Edward F. Gehringer, Department of Electrical and Computer Engineering Department of Computer Science North Carolina State University efg@ncsu.edu Choosing Passwords: Security and Human Factors

[76] DeAlvare, A.M. A framework for password selection. In Proceedings of Unix Security Workshop II. (Portland, Aug. 29–30, 1998).

[77] DeAlvare, A.M. How crackers crack passwords or what passwords to avoid. In Proceedings of Unix Security Workshop II. (Portland, 1990)

[78] Addison Wesley Real 802.11 Security: Wi-Fi Protected Access and 802.11i

[79] FIPS. Password Usage. Federal Information Processing Standards Publication. May 30, 1985.

[80] Patrick Manzo Adhikari, November 21, 2008Officer Monster Worldwide , January 23, 2009 [Online] http://help.monster.com/besafe/jobseeker/index.asp

[81] Karen Kent, Murugiah Souppaya Guide to Computer Security Log Management

[82] Babbin, Jacob et al, Security Log Management: Identifying Patterns in the Chaos, Syngress, 2006.

[83] Bauer, Michael D., Chapter 10 (System Log Management and Monitoring) of Building Secure

[84] Servers with LINUX, O'Reilly, 2002. Giuseppini, Gabriele, Microsoft Log Parser Toolkit, Syngress, 2005.

[85] Maier, Phillip Q., Audit and Trace Log Management: Consolidation and Analysis, Auerbach, 2004.

[86] Osborne, Mark. How to Cheat at Managing Information Security. Rockland, MA, USA: Syngress Publishing, 2006. p 56.

[87] USERS ARE NOT THE ENEMY Anne Adams (A.Adams@cs.ucl.ac.uk) is a Ph.D. candidate in the

Department of Computer Science at the University College of London. Martina Angela Sasse (A.Sasse@cs.ucl.ac.uk) is Senior Lecturer in the Department of Computer Science at the University College of London.

[88] Richard Sheiman, "A balanced approach to information security" [Online] http://www.infoscreen.com/publications/InfoScreen_balanced_approach.pdf,

[89] SYMANTEC,"Behind the Firewall – The Insider Threat: Part II" [Online] http://enterprisesecurity.symantec.com/article.cfm?articleid=2160&EID=0

[90] Wendy Arthurs, "A proactive defence to Social Engineering" [Online] http://www.sans.org/rr/paper.php?id=511,

[91] Nate Anderson Senior Editor.Published: September 16, 2007 - 11:19PM CT Insiders cause more computer security problems than viruses [Online] http://arstechnica.com/news.ars/post/20070916-report-insiders-cause-more-computer-security-problems-than-viruses.html

[92] Definitions. March 21,2009 [Onilne] http://www.yourwindow.to/information-security http://www.wikipedia.org/

[93] Wendy Arthurs, "A proactive defence to Social Engineering" [Online] http://www.sans.org/rr/paper.php?id=511,

[94] Radha Gulati, "The Threat of Social Engineering and Your Defence Against It" [Online] http://www.sans.org/rr/papers/index.php?id=1192,

[95] Japan: Arrests Made in Softbank Data Leak Case, 01 June 2004. [On-line] Retrieved. November 30, 2004 at URL: http://www.theregister.co.uk/2004/06/01/softbank_dat_leak/

[98] Configuration Management Guide, DOE CIO Guidance CS-8 www.hackemate.com.ar/advisories/SecurityFocus% 20Microsoft%20Newsletter/SecurityFocus%20Microsoft%20Newsletter%20071.txt

[100] Peter Burkholder, February 1, 2002 (v2.0) SSL Man-in-the-Middle Attacks

[101] INTERLINK Networks [Online] http://www.lucidlink.com/media/pdf_autogen/Link_and_Network_Layer_Whitepaper.pdf

[102] UCSD policy and procedure manual,computing services Security for electronic information at UCSD

[103] Users Are Not The Enemy, COMMUNICATIONS OF THE ACM December 1999/Vol. 42, No. 12

[104] Communication Technologies, Inc. TECHNICAL INFORMATION BULLETIN 04-1 Supervisory Control and Data Acquisition (SCADA) Systems

[105] Singer, Abe and Bird, Tina, Building a Logging Infrastructure, USENIX Association, 2004

[106] Richard Barber, "Social Engineering: A people problem?"
Network security, volume 2001.

[107] Bernadette H. Schell and Clemens Martin, CYBERCRIME: A REFERENCE HANDBOOK
Cybercrime: Incident Response and Digital Forensics [Online]
http://searchsecurity.techtarget.com/searchSecurity/downloads/Cybercrime_Ch2.pdf

[108] Anton, Philip S.; Anderson, Robert H.; Mesic, Richard. Finding and Fixing Vulnerabilities in Information Systems : The Vulnerability Assessment and Mitigation Methodology.
Santa Monica, CA, USA: Rand Corporation, The, 2003. p 53.

[109] Security+ Study Guide
By Michael Cross, Norris L. Johnson, Tony Piltzecker
[110] Computer Network II, By V.S. Bagad, I.A. Dhotre

[111] http://www.cisco.com/warp/public/707/cisco-sa-19971121-land.shtml

[112] Online http://www.securityfocus.com/infocus/1783

[113] Hacking Wireless Networks
By Kevin Beaver, Peter T. Davis

[114] Ghosh, Sumit (Editor); Malek-Zavarei, Manu (Editor); Stohr, Edward A. (Editor). Guarding Your Business : A Management Approach to Security.
Hingham, MA, USA: Kluwer Academic Publishers, 2004. p 121.

[115] Anton, Philip S.; Anderson, Robert H.; Mesic, Richard. Finding and Fixing Vulnerabilities in Information Systems : The Vulnerability Assessment and Mitigation Methodology.
Santa Monica, CA, USA: Rand Corporation, The, 2003. p 56.

[116] Cannon, David L.; Melber, Derek; Bergmann, Timothy S.. CISA : Certified Information System Auditor Study Guide.
Alameda, CA, USA: Sybex, Incorporated, 2006. p 285.
[117] Stewart, J. M.; Tittle, Ed; Chapple, Mike. CISSP Professional : Certified Information Systems Security Professional Study Guide. Alameda, CA, USA: Sybex, Incorporated, 2005. p 268

[118] Maiwald, Eric. Network Security : A Beginner's Guide.
Blacklick, OH, USA: McGraw-Hill Professional, 2002. p 398.

[119] Ghosh, Sumit (Editor); Malek-Zavarei, Manu (Editor); Stohr, Edward A. (Editor). Guarding Your Business : A Management Approach to Security.
Hingham, MA, USA: Kluwer Academic Publishers, 2004. p 39.

[120] Wallace, Michael; Webber, Lawrence. Disaster Recovery Handbook.
New York, NY, USA: AMACOM, 2004. p 90.
[121]Wallace, Michael; Webber, Lawrence. Disaster Recovery Handbook.
New York, NY, USA: AMACOM, 2004. p 76.
[122] IBM Redbooks. Content Manager OnDemand Backup, Recovery, and High Availability.
Durham, NC, USA: IBM, 2005. p 24.

10 APPENDIX A: SURVEY

10.1.1 List of Mistakes

Sr No	Mistakes
1	Firewalls, IDS, Routers and Switches are misconfigured
2	Installation and configuration of operating system and software used in SCADA and/or corporate network are not completed correctly
3	Unneeded Ports and services remain open after installation of operating system or application??
4	Wireless links in computer network are misconfigured
5	Default setting/values of devices are not changed when configuring
6	System maintenance, modification and testing are not completed correctly
7	Access control policies in computer networks are not implemented correctly
8	Taking and restoration of backups are completed incorrectly
9	Updates and Patches of OS, Antivirus and firmware are not manage properly
10	Supporting services or facilities not managed properly
11	Peripheral Devices are not managed properly
12	Strong password policy not implemented e.g. minimum password length, use of alpha-numeric and special characters
13	Password is written down on paper by user incase of strong password
14	Log management e.g. Proper Backup and reading of logs generated by system and devices) are not completed properly
15	Sensitive information from Technical Staff disclosed by means of social engineering

10.1.2 Questionnaire Phase I, List of Causes

Following are the types of questions that were asked to administrators, operators and security experts.

I am Muhammad Afzal. I am a student of MS (Information and Communication System Security) at KTH (The Royal Institute of Technology), Stockholm, SWEDEN. This interview is a part of my Master Thesis work, which is "Human and Organization aspect of Cyber Security"
The purpose of this interview is to collect possible causes of mistakes in Information System because of Human negligence.
Your help will be valuable for me. Thank you in advance!

1. What are the major factors that influence if Firewalls, IDS, Routers and Switches are misconfigured? (e.g. Complexity)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	Low Education level	2	Lack of coordination
3	Structure Design	4	Different Hardware
5	New Software	6	Works stress
7	Sloppiness	8	Inadequate Instructions
Respondent B			
9	Too complex NW	10	Setup is don early before customer knows what he wants
11	Changes during implementation, ports left open		
Respondent C			
12	Lack of education	13	Resources workload
14	Resource priority	15	Equipment not available provided by client
16	Complexity	17	Parts of HW deliver by client
Respondent D			
18	Insufficient training	19	Ignorance
20	Unknown requirements		
Respondent E			
21	Insufficient documentation	22	Not enough timings
23	Misunderstanding of customer requirement	24	No standardized equipment different for different project
Respondent F			
25	Competency	26	No clear view what to stop and what to let through

2. What are the major factors that influence if installation and configuration of operating system and software used in SCADA and/or corporate network are not don correctly?
(e.g. Work Stress)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	Low Education level	2	Lack of coordination
3	Structure Design	4	Works stress
5	New Software		
Respondent B			
6	Setup is don early before customer knows what he wants	7	Inadequate Instructions
8	Sloppiness	9	Sloppiness
Respondent C			
10	Lack of instruction	11	Low Patch level knowledge
12	Different hardware (dell, IBM, HP etc)		
Respondent D			
13	Insufficient training	14	Cost
15	Insufficient, missing process	16	Policies
17	Ignorance		
Respondent E			
18	Insufficient documentation	19	Templates for this is not used
20	No configuration decided		
Respondent F			
21	Stress	22	No clear view of exact need

3. What are the major factors that influence due to keep unwanted ports and services open after installation of operating system or any new service?
(e.g. Technical Potential)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	To Ease in Handling Software	2	Changes during implementation, ports left open
3	No understanding Security	4	Incomplete installation guide
5	Complexity of System	6	Test situation force to open, forget to close afterwards
Respondent B			
7	not aware of all required services, better leave it open.	8	Easy access to ABB personal
9	Setup is don early before customer knows what he wants		
Respondent C			
10	Inappropriate Instruction guide	11	Window template missing
Respondent D			
12	Unknown requirement	13	Insufficient training
Respondent E			
14	Lack of knowledge of importance	15	Documentation not available how to use ports
Respondent F			
16	Exact need not documented	17	Easy to have open for installation

4. What are the major factors that influence if wireless links in computer network are misconfigured? (e.g. Technical Potential)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	Low Education level	2	Sloppiness
3	Structure Design	4	Inadequate Instructions

5	Works stress		
Respondent B			
6	NA		
Respondent C			
1	NA		
Respondent D			
8	Insufficient training	9	Ignorance
10	Insufficient policies		
Respondent E			
11	NA		
Respondent F			
13	Open access to easier in installation		

5. What are the major factors that influence if Default setting/values of devices are not changed when configuring?
   (e.g. Work Stress)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	Sloppiness	2	Works stress
3	Inadequate Instructions		
Respondent B			
4	Incomplete installation guides	5	No knowledge about setup
6	Work stress		
Respondent C			
7	Lack of instruction	8	Time at hand
Respondent D			

9	Ignorance		
Respondent E			
10	Insufficient documentation	11	No enough timings
12	Not standardized equipment different for different projects	13	Too much trial and error work
Respondent F			
14	Stress	15	Culture routine
16	Lack of documentation or to complicated description		

6. What are the major factors that influence if System maintenance, modification and testing are not completed correctly?
(e.g. Installation guide is not updated)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	Low Education level	2	Time to test and implement instruction
3	New Software	4	Different Hardware
5	Sloppiness	6	Works stress
Respondent B			
7	Incomplete document	8	Do not know better
Respondent C			
9	Complexity	10	Update process is not ok
11	Lack of testing environment	12	Lack of understanding security
Respondent D			
13	Time	14	Cost
Respondent E			
15	Lack of time to investigate unexpected behavior of the system	16	Lack of predefined procedures

17	Lack of imagination	18	Engineers are familiar which go wrong the system
Respondent F			
19	Specification not evaluated with upgrades and maintenance in mind	20	Increased ambition during implementation
21	Lack of time to test	22	Documents not updated

7. What are the major factors that influence if access control policies in computer networks are not implemented correctly?
(e.g. Misunderstanding)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	Low Education level	2	Lack of coordination
3	Sloppiness	4	Works stress
5	Inadequate Instructions		
Respondent B			
6	Setup is don early before customer knows what he wants	7	Changes during implementation, ports left open
8	Too complex NW		
Respondent C			
9	Tradition, easiness	10	Lack of NM functionality
11	Policy guidelines missing		
Respondent D			
12	Unknown potential	13	Ignorance
14	Insufficient training		
Respondent E			
15	Lack of time	16	Lack of education
17	Lack of policy what to allow	18	Misunderstanding between ABB and client

Respondent F			
19	Lack of clear vision	20	To complicated configuration

8. What are the major factors that influence while taking and restoration of backups don incorrectly? (e.g. Importance of Backups)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	Low Education level	2	Inadequate Instructions
3	New Software		
Respondent B			
4	Hard to know how to do it	5	Hard to setup a schedule for automatic backup
6	Customer responsibility	7	Documentation
8	No one responsible		
Respondent C			
9	Tool complexity	10	No preferred backup tool
11	Understanding		
Respondent D			
12	Erroneous implementation	13	Erroneous Procedure
14	Incomplete scope	15	Unknown requirement
Respondent E			
16	Lack of documentation how to do it	17	Lack of knowledge
18	No understanding of importance		
Respondent F			
19	Backup not taken after until something not happen	20	Test of restore not don

9. What are the major factors that influence if updates of OS, Antivirus and firmware are not managed properly?
(e.g. Lack of Policy)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	Inadequate Instructions		
Respondent B			
2	Customer policy not established	3	No personnel is responsible
Respondent C			
4	Update policy missing		
5	Lack of test environment		
Respondent D			
6	Cost	7	Time
8	Unknown requirement	9	Insufficient policies
Respondent E			
10	Lack of policy	11	No understanding of the importance
12	Afraid to do this, system might not work	13	Equipment unavailability to test before deployment
Respondent F			
14	Lack of test environment	15	Lack of policy
16	Nothing has happens		

10. What are the major factors that influence if supporting services or facilities like heating or cooling (AC), electricity etc not managed properly? For example: power failure can cause loss in availability due to computer and peripheral failure.
(e.g. Improper Network Architecture)

Sr. No	Factors	Sr. No	Factors

Respondent A			
1	Structure Design	2	Inadequate Instructions
3	Sloppiness	4	Lack of coordination
Respondent B			
5	Customer responsibility	6	No routines in place UPS
7	Not tested regularly		
Respondent C			
8	Lack of redundant architecture		
Respondent D			
9	Unknown requirement	10	Insufficient implementation
11	Incomplete scope	12	Cost
Respondent E			
13	Lack of equipment maintenance	14	No procedures for the maintenance
Respondent F			
15	No maintenance procedures		

11. What are the major factors that influence if removable media is permitted in the network? (e.g. Lack of Security Policy)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	Sloppiness	2	No understanding of Security
3	Inadequate Instructions	4	Easy to Handle
Respondent B			
5	Lack of security policy	6	Convenience

Respondent C			
7	Virus threats		
Respondent D			
8	Missing requirement	9	Unknown potential
10	Missing policy		
Respondent E			
11	Lack of awareness of the cyber security threats	12	Convenient to use
Respondent F			
13	No policy	14	Easy in use / information movement is easy

12. What are the major factors that influence if Strong password policy not implemented e.g. minimum password length, use of alpha-numeric and special characters?
(e.g. User reuse to accept it)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	User ease	2	Help Desk Work Stress
3	No Security Policy		
Respondent B			
4	Lack of security implementation	5	Simplicity
Respondent C			
6	Tradition	7	Lack of understanding
8	Convenience	9	Easiness
10	Lack of instruction		
Respondent D			
11	Insufficient enforcement	12	Missing technology
13	Insufficient training	14	Cost

Respondent E			
15	Security awareness	16	IT policy
Respondent F			
17	User / operators find it difficult and time consuming	18	Inconveniences

13. What are the major factors that influence if password is written down on paper by user incase of strong password?
(e.g. Excessively Complicated Combination)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	Hard to Remember	2	No Understanding of Security
3	Several Passwords	4	Sloppiness
Respondent B			
5	'Excessively complicated combination	6	Too much password to remember
Respondent C			
7	Not to forgot	8	Some time need to written down due to documentation
Respondent D			
9	Humanity		
Respondent E			
10	No awareness	11	Old traditions to cut corners
12	Sloppy culture among people	13	Complex password not easy to remember
Respondent F			
14	Many different password difficult to remember	15	No policy against borrowing between operators

14. What are the major factors that influence if log management e.g. Proper Backup and reading of logs generated by system and devices) are not completed properly?
(e.g. Shortage of Technical Staff/no one take responsibility)

Sr. No	Factors	Sr. No	Factors
Respondent A			
1	Work stress	2	Inadequate Instructions
3	Low Education level		
Respondent B			
4	Shortage of technical staff	5	No one take responsibility
6	Policy missing		
Respondent C			
7	Lack of understanding	8	Lack of instruction
Respondent D			
9	Unknown requirements	10	Unknown potential
11	Insufficient training	12	Ignorance
13	Missing technology		
Respondent E			
14	Sloppiness	15	Lack of procedures
16	Lack of responsibility and organization		
Respondent F			
17	No one has the responsibility	18	Lack of time
19	Importance		

15. What are the major factors that influence if sensitive information from Technical Staff disclosed by means of social engineering?
(e.g. Deception)

Sr. No	Factors	Sr. No	Factors
Respondent A			

1	Same computer access Internet	2	Impersonating
Respondent B			
3	Policy of company	4	Person not aware of it
Respondent C			
5	Party	6	Bragging
Respondent D			
7	Insufficient training	8	Ignorance
Respondent E			
9	Employees are unhappy	10	No awareness of social engineering threats
11	Fake emails and web pages etc		
Respondent F			
11	Thoughtlessness	12	Anger not satisfied with employer

10.1.3 Questionnaire Phase I, Grouping of Similar Causes

1. What are the major causes that influence if Firewalls, IDS, Routers and Switches are misconfigured? (e.g. Complexity)

Sr. No	Causes	Ranking	Common Factor
1	Low Education level	1	Lack of education/Competency and training
2	Lack of education		
3	Insufficient training		
4	Competency		
5	No clear view what to stop and what to let through		
6	Carelessness		
7	Ignorance		
8	Structure Design	2	Complexity in structure/hardware/design/changes in the configuration
9	Too complex NW		
10	Complexity		
11	Changes in Software configuration		
12	Different Hardware		
13	No standardized equipment different for different project		
14	Changes during implementation, ports left open	3	Lack of requirements engineering/poor documentation
15	Lack of coordination		

16	Misunderstanding of customer requirement		
17	Unknown requirements		
18	Insufficient documentation		
19	Inadequate Instructions		
20	Setup is completed early before customer knows what he wants		
21	Not enough timings	4	Insufficient resources
22	Resources workload		
23	Works stress		
24	Resource priority		
25	Equipment not available provided by client		
26	Parts of HW deliver by client		

2. What are the major causes that influence if installation and configuration of operating system and software used in SCADA and/or corporate network are not completed correctly?
(e.g. Work Stress)

Sr. No	Causes	Ranking	Common Factor
1	Low Education level	1	Lack of education/Competency and training
2	Low Patch level knowledge		
3	Insufficient training		
4	Templates for this is not used		
5	Sloppiness		

6	Carelessness		
7	Ignorance		
8	Structure Design	2	Complexity in structure/hardware/design/changes in the configuration
9	Changes in Software configuration		
10	Different hardware (dell, IBM, HP etc)		
11	Lack of coordination	3	Lack of requirements engineering/poor documentation
12	Setup is completed early before customer knows what he wants		
13	Lack of instruction		
14	Insufficient documentation		
15	Policies		
16	Inadequate Instructions		
17	No configuration decided		
18	No clear view of exact need		
19	Works stress	4	Insufficient resources
20	Stress		

3. What are the major causes that influence due to keep unwanted Unneeded Ports and services remain open after installation of operating system or application?? (e.g. Technical Potential)

Sr. No	Causes	Ranking	Common Factor
1	Setup is completed early before customer knows what he wants	1	Lack of requirements engineering / poor documentation
2	Unknown requirement		
3	Exact need not documented		
4	Incomplete installation guide		

5	Inappropriate Instruction guide		
6	Documentation not available how to use ports		
7	To Ease in Handling Software	2	Ignorance in following proper procedure for personal ease
8	Easy access to personal		
9	Easy to have open for installation		
10	Complexity of System	3	Complexity in structure/hardware/design/changes in the configuration
11	Changes during implementation, ports left open		
12	Test situation force to open, forget to close afterwards		
13	Lack of knowledge of importance	4	Lack of education/Competency and training
14	No understanding Security		
15	Insufficient training		
16	not aware of all required services, better leave it open.		
17	Window template missing		

4. What are the major causes that influence ifWireless links in computer network are misconfigured? (e.g. Technical Potential)

Sr. No	Causes	Ranking	Common Factor
1	Inadequate Instructions	1	Insufficient documentation/policies
2	Insufficient policies		
3	Open access to easier in installation		
4	Low Education level	2	Lack of education/Competency and training
5	Carelessness		
6	Ignorance		
7	Insufficient training		
8	Structure Design	3	Complexity in structure/hardware/design/changes in the

			configuration
9	Works stress	4	Less resources

5. What are the major causes that influence if Default setting/values of devices are not changed when configuring? (e.g. Work Stress)

Sr. No	Causes	Ranking	Common Factor
1	No knowledge about setup	1	Lack of education/Competency and training
2	Lack of documentation or too complicated description		
3	Culture routine		
4	Carelessness		
5	Too much trial and error work		
6	Ignorance		
7	Inadequate Instructions	2	Improper instructions guide
8	Incomplete installation guides		
9	Lack of instruction		
10	Insufficient documentation		
11	Not standardized equipment different for different projects	3	System complexity

12	Stress	4	Insufficient resources
13	Time at hand		
14	Work stress		
15	No enough timings		

6. What are the major causes that influence if System maintenance, modification and testing are not completed correctly? (e.g. Installation guide is not updated)

Sr. No	Causes	Ranking	Common Factor
1	Time to test and implement instruction	1	Insufficient resources
2	Lack of testing environment		
3	Time		
4	Lack of time to investigate unexpected behavior of the system		
5	Lack of time to test		
6	Increased ambition during implementation		
7	Works stress		
8	Cost		
9	Different Hardware	2	Complexity in structure/hardware/design
10	Changes in Software configuration		
11	Complexity		
12	Incomplete document	3	Poor documentation
13	Update process is not ok		

14	Lack of predefined procedures		
15	Documents not updated		
16	Low Education level	4	Lack of education/Competency and training
17	Do not know better		
18	Lack of understanding security		
19	Lack of imagination		
20	Specification not evaluated with upgrades and maintenance in mind		
21	Engineers are not familiar which go wrong the system		
22	Carelessness		

7. What are the major causes that influence if access control policies in computer networks are not implemented correctly? (e.g. Misunderstanding)

Sr. No	Causes	Ranking	Common Factor
1	Changes during implementation	1	Lack of requirements engineering / poor documentation
2	Lack of coordination		
3	Misunderstanding between solution provider and client		
4	Setup is completed early before customer knows what he wants		
5	Lack of policy what to allow		
6	Inadequate Instructions		
7	Policy guidelines missing		
8	Low Education level	2	Lack of education/Competency and training
9	Unknown potential		
10	Insufficient training		
11	Lack of clear vision		

12	Lack of education		
13	Tradition, easiness		
14	Carelessness		
15	Ignorance		
16	Too complex NW	3	Complexity in network structure and design
17	To complicated configuration		
18	Works stress	4	Insufficient resources
19	Lack of time		
20	Lack of NM functionality		

8. What are the major causes that influence while Taking and restoration of backups are completed incorrectly?
(e.g. Importance of Backups)

Sr. No	Causes	Ranking	Common Factor
1	Low Education level	1	Lack of education/Competency and training
2	Understanding		
3	Lack of knowledge		
4	Hard to know how to do it		
5	Hard to setup a schedule for automatic backup		
6	New Software		
7	Erroneous Procedure		
8	Erroneous implementation		
9	Incomplete scope	2	Lack of requirements engineering / poor documentation
10	Unknown requirement		
11	Documentation		
12	Inadequate Instructions		
13	Lack of documentation how to do it		

15	Responsibility	3	Importance
16	No one responsible		
17	No understanding of importance		
18	Backup not taken after until something not happen		
19	No preferred backup tool	4	Resource unavailable
20	Test of restore not completed		

9. What are the major causes that influence if updates and patches of OS, Antivirus and firmware are not managed properly? (e.g. Lack of Policy)

Sr. No	Causes	Ranking	Common Factor
1	Inadequate Instructions	1	Insufficient policies/requirement
2	Lack of policy		
3	Customer policy not established		
4	Update policy missing		
5	Lack of policy		
6	Insufficient policies		
7	Unknown requirement		
8	Afraid to do this, system might not work		
9	No personnel is responsible	2	Importance/carelessness

10	No understanding of the importance		
11	Equipment unavailability to test before deployment	3	Insufficient Resources
12	Lack of test environment		
13	Lack of test environment		
14	Time		
15	Cost		

10. What are the major causes that influence if supporting services or facilities like heating or cooling (AC), electricity etc not managed properly? For example: power failure can cause loss in availability due to computer and peripheral failure. (e.g. Improper Network Architecture)

Sr. No	Causes	Ranking	Common Factor
1	Unknown requirement	1	Improper requirements
2	Incomplete scope		
3	Insufficient implementation	2	Lack of education/Competency and training
4	No procedures for the maintenance		
5	Not tested regularly		
6	No maintenance procedures		
7	Customer responsibility		
8	Carelessness		
9	No routines in place UPS		
10	Lack of equipment maintenance	3	Insufficient resources
11	Lack of redundant architecture		

12	Cost		
13	Structure Design		

11. What are the major causes that influence if Peripheral Devices are not managed properly?
(e.g. Lack of Security Policy)

Sr. No	Causes	Ranking	Common Factor
1	Lack of awareness of the cyber security threats	1	Lack of education/Competency and training
2	No understanding of Security		
3	Carelessness		
4	No policy	2	Poor documentation/policies
5	Missing policy		
6	Inadequate Instructions		
7	Missing requirement		
8	Lack of security policy		
9	Easy to Handle	3	User ease
10	Convenience		
11	Convenient to use		
12	Unknown potential		
13	Easy in use / information movement is easy		

12. What are the major causes that influence if Strong password policy not implemented e.g. minimum password length, use of alpha-numeric and special characters?
(e.g. User reuse to accept it)

Sr. No	Causes	Ranking	Common Factor
1	No Security Policy	1	Poor documentation / policies
2	Lack of instruction		
3	IT policy		
4	Simplicity	2	User ease

5	User ease		
6	Tradition		
7	Convenience		
8	Easiness		
8	User / operators find it difficult and time consuming		
10	Help Desk Work Stress		
11	Lack of understanding	3	Lack of education/Competency and training
12	Lack of security implementation		
13	Insufficient enforcement		
14	Insufficient training		
15	Security awareness		

13. What are the major causes that influence if password is written down on paper by user incase of strong password? (e.g. Excessively Complicated Combination)

Sr. No	Causes	Ranking	Common Factor
1	Hard to Remember	1	Complexity/Low level education/importance
2	Several Passwords		
3	Too much password to remember		
4	Not to forgot		
5	Humanity		
6	Old traditions to cut corners		
7	Complex password not easy to remember		
8	Many different password difficult to remember		
9	Excessively complicated combination		

10	No policy against borrowing between operators	2	Poor documentation /policies
11	Some time need to written down due to documentation		
12	No Understanding of Security	3	Lack of education/Competency and training
13	Carelessness		
14	No awareness		
15	Sloppy culture among people		

14. What are the major causes that influence if log management e.g. Proper Backup and reading of logs generated by system and devices) are not completed properly?
(e.g. Shortage of Technical Staff/no one take responsibility)

Sr. No	Causes	Ranking	Common Factor
1	Unknown requirements	1	Lack of requirement / poor documentation
2	Unknown potential		
3	Missing technology		
4	Inadequate Instructions		
5	Lack of instruction		
6	Policy missing		
7	Work stress	2	Lack of education/Competency and training
8	Low Education level		
9	Lack of understanding		

10	Lack of procedures		
11	Insufficient training		
12	Carelessness		
13	Ignorance		
14	No one take responsibility	3	Insufficient resources
15	Shortage of technical staff		
16	Lack of responsibility and organization		
17	No one has the responsibility		
18	Importance		
19	Lack of time		

15. What are the major causes that influence if sensitive information from Technical Staff disclosed by means of social engineering? (e.g. Deception)

Sr. No	Causes	Ranking	Common Factor
1	Person not aware of it	1	Lack of education/Competency and training
2	Party		
3	Insufficient training		
4	No awareness of social engineering threats		
5	Thoughtlessness		
6	Ignorance		
7	Fake emails and web pages etc		

8	Impersonating		
9	Policy of company	2	Missing policy
10	Same computer access Internet		
11	Employees are unhappy	3	Employees not satisfied
12	Anger not satisfied with employer		

10.1.4 Compilation of Questionnaire Phase I

Sr No	Mistakes	Common Causes	Causes of Interest
1	Firewalls, IDS, Routers and Switches are misconfigured?	Complexity in structure/hardware/design/changes in the configuration	Complexity in structure/hardware/design/changes in the configuration Lack of requirements engineering/poor documentation Lack of education/Competency and training Insufficient resources Ignorance in following proper procedure for personal ease Improper instructions guide/ Policies Importance/carelessness User ease Complexity in policy Employees not satisfied
		Lack of requirements engineering/poor documentation	
		Lack of education/Competency and training	
		Insufficient resources	
2	Configuration of operating system and software used in SCADA and/or corporate network are not done correctly?	Complexity in structure/hardware/design/changes in the configuration	
		Lack of requirements engineering/poor documentation	
		Lack of education/Competency and training	
		Insufficient resources	
3	Unneeded Ports and services remain open after installation of operating system or application??	Complexity in structure/hardware/design/changes in the configuration	
		Lack of requirements engineering/poor documentation	
		Lack of education/Competency and training	
		Ignorance in following proper procedure for personal ease	
4	Wireless links in computer network are misconfigured?	Complexity in structure/hardware/design/changes in the configuration	
		Improper instructions guide/ Policies	
		Lack of education/Competency and training	
		Insufficient resources	
5		Complexity in Structure/hardware/design/changes in the configuration	

	Default setting/values of devices are not changed when configuring?	Improper instructions guide/ Policies	
		Lack of education/Competency and training	
6	System maintenance, modification and testing are not completed correctly?	Complexity in structure/hardware/design/changes in the configuration	
		Improper instructions guide/ Policies	
		Lack of education/Competency and training	
		Insufficient resources	
7	Access control policies in computer networks are not implemented correctly?	Complexity in structure/hardware/design/changes in the configuration	
		Lack of requirements engineering/poor documentation	
		Lack of education/Competency and training	
		Insufficient resources	
8	Taking and restoration of backups don incorrectly?	Lack of education/Competency and training	
		Insufficient resources	
		Importance/carelessness	
9	Updates and Patches of OS, Antivirus and firmware are not managed properly?	Improper instructions guide/ Policies	
		Insufficient resources	
		Importance/carelessness	
10	Supporting services or facilities not managed properly?	Lack of requirements engineering/poor documentation	
		Lack of education/Competency and training	

		Insufficient resources	
11	Peripheral Devices are not managed properly?	Improper instructions guide/ Policies	
		Lack of education/Competency and training	
		User ease	
12	Strong password policy not implemented e.g. minimum password length, use of alpha-numeric and special characters?	Improper instructions guide/ Policies	
		Lack of education/Competency and training	
		User ease	
13	Password is written down on paper by user incase of strong password?	Improper instructions guide/ Policies	
		Lack of education/Competency and training	
		Complexity in policy	
		Importance/carelessness	
14	Log management e.g. Proper Backup and reading of logs generated by system and devices) are not completed properly?	Lack of education/Competency and training	
		Insufficient resources	
		Importance/carelessness	
15	Sensitive information from Technical Staff disclosed by means of social engineering?	Lack of education/Competency and training	
		Employees not satisfied	

10.2 Questionnaire Phase II, Priority/Ranking of Causes

What percentage of projects does the following condition apply?

Ranking	Causes	Probabilities						
		Respondent-A	Respondent-B	Respondent-C	Respondent-D	Respondent-E	Respondent-F	Average
1	Complexity in structure/hardware/design/changes in the configuration	100	90	50	50	50	40	**63.33**
2	Improper instructions guide/ Policies	70	80	99	20	15	45	**54.83**
3	Lack of requirements engineering/poor documentation	40	30	60	70	20	45	**44.16**
4	Lack of education/Competency and training	20	10	20	80	60	45	**39.16**
5	Ignorance in following proper procedure for personal ease	10	10	80	70	10	50	**38.33**
6	Insufficient resources	60	50	40	5	30	40	**37.5**
7	Complexity in policy	30	20	70	15	10	35	**30**
8	User ease	10	10	70	7	10	30	**22.83**
9	Importance/carelessness	10	5	10	30	5	35	**15.83**
10	Employees not satisfied	20	10	5	2	5	10	**8.66**

10.3 Questionnaire Phase III, Conditional Probability Table

CPT – 1

Firewalls, IDS, Routers and Switches are misconfigured?	Complexity in structure/hardware/design/changes in the configuration	T								F							
	Lack of requirements engineering/poor documentation	T				F				T				F			
	Lack of education/Competency and training	T		F		T		F		T		F		T		F	
	Insufficient resources	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	90	85	80	55	50	45	15	90	80	65	60	75	70	20	0
Respondent-B	TRUE	100	90	70	50	85	75	60	20	80	65	50	45	60	65	30	0
Respondent-C	TRUE	100	95	60	65	65	45	40	10	95	70	65	35	60	50	15	0
Respondent-D	TRUE	100	99	45	55	85	84	35	10	95	85	40	25	75	65	15	0
Respondent-E	TRUE	90	80	70	60	75	65	65	35	80	70	60	50	55	50	25	5
Respondent-F	TRUE	95	90	85	70	90	60	40	20	75	70	65	50	65	45	15	0
Respondent-G	TRUE	100	95	70	65	90	80	65	15	95	80	70	65	45	40	10	5
Respondent-H	TRUE	100	95	75	85	85	80	70	45	65	65	55	45	55	50	10	0
MEAN VALUE		98.13	91.75	70	66.25	78.75	67.38	52.5	21.25	84.38	73.13	58.75	46.88	61.25	54.38	17.5	1.25
MAD (Mean Absolute Deviation)		2.8125	4.25	8.75	9.0625	10.313	12.375	12.5	9.375	9.375	6.4063	7.8125	9.375	7.8125	9.2188	5.625	1.875

CPT – 2

Installation and configuration of operating system and software used in SCADA and/or corporate network are not completed correctly?	Complexity in structure/hardware/design/changes in the configuration	T								F							
	Lack of requirements engineering/poor documentation	T				F				T				F			
	Lack of education/Competency and training	T		F		T		F		T		F		T		F	
	Insufficient resources	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	95	75	70	70	45	45	30	70	60	60	40	45	30	5	0
Respondent-B	TRUE	100	80	60	45	80	75	50	25	65	50	45	35	50	40	30	0
Respondent-C	TRUE	100	90	75	75	70	45	40	20	80	55	60	50	40	35	10	0
Respondent-D	TRUE	100	95	45	55	50	45	20	17	90	80	35	20	60	55	13	1
Respondent-E	TRUE	99	95	80	75	90	75	55	45	95	85	65	55	65	55	20	0
Respondent-F	TRUE	95	90	85	70	90	60	45	20	75	70	65	50	70	40	10	0
Respondent-G	TRUE	100	95	70	65	85	80	65	25	85	70	75	55	45	30	10	5
Respondent-H	TRUE	100	95	80	75	80	80	60	35	65	65	55	50	40	25	10	0
MEAN VALUE		99.25	91.88	71.25	66.25	76.88	63.13	47.5	27.13	78.13	66.88	57.5	44.38	51.88	38.75	13.5	0.75
MAD (Mean Absolute Deviation)		1.125	3.90625	9.6875	8.4375	10.1563	14.375	10	7.15625	9.375	9.375	9.375	9.53125	9.84375	8.75	5.75	1.125

CPT – 3

Unneeded Ports and services remain open after installation of operating system or application??	Complexity in structure/hardware/design/changes in the configuration	T								F							
	Lack of requirements engineering/poor documentation	T				F				T				F			
	Lack of education/Competency and training	T		F		T		F		T		F		T		F	
	Ignorance in following proper procedure for personal ease	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	95	95	85	65	50	45	30	90	80	70	65	45	25	5	0
Respondent-B	TRUE	100	100	90	70	80	45	50	30	100	90	65	60	55	30	20	0
Respondent-C	TRUE	100	90	90	80	75	55	40	25	90	65	55	60	40	25	10	0
Respondent-D	TRUE	100	95	95	90	55	45	30	25	90	85	75	75	40	35	20	15
Respondent-E	TRUE	100	90	80	70	75	60	55	15	100	85	70	50	65	45	35	0
Respondent-F	TRUE	100	90	85	70	90	75	60	50	80	70	65	45	50	35	20	0
Respondent-G	TRUE	100	85	75	65	60	50	45	30	80	65	50	55	60	40	20	10
Respondent-H	TRUE	100	95	95	90	85	75	65	45	65	60	50	40	40	25	10	0
MEAN VALUE		100	92.5	88.13	77.5	73.13	56.88	48.75	31.25	86.88	75	62.5	56.25	49.38	32.5	17.5	3.125
MAD (Mean Absolute Deviation)		0	3.75	6.0938	8.75	9.8438	9.8438	8.75	8.125	8.9063	10	8.125	8.75	8.125	6.25	6.875	4.6875

CPT – 4

Wireless links in computer network are misconfigured?	Complexity in structure/hardware/design/changes in the configuration	T								F							
	Improper instructions guide/ Policies	T				F				T				F			
	Lack of education/Competency and training	T		F		T		F		T		F		T		F	
	Insufficient resources	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	90	85	75	55	50	40	20	90	80	55	65	30	25	15	0
Respondent-B	TRUE	100	90	75	55	75	45	45	25	90	80	60	50	40	30	25	0
Respondent-C	TRUE	100	95	85	75	60	55	50	20	85	75	55	65	35	25	10	0
Respondent-D	TRUE	95	95	65	60	60	60	45	20	80	80	55	55	45	45	15	5
Respondent-E	TRUE																
Respondent-F	TRUE	100	85	80	60	75	65	55	30	70	70	50	50	40	30	20	0
Respondent-G	TRUE	100	95	70	65	75	60	65	25	95	85	65	65	35	35	15	5
Respondent-H	TRUE	100	95	90	80	80	65	65	40	65	70	55	50	30	25	10	0
MEAN VALUE		99.2857143	92.1428571	78.5714286	67.1428571	68.5714286	57.1428571	52.1428571	25.7142857	82.1428571	77.1428571	56.4285714	57.1428571	36.4285714	30.7142857	15.7142857	1.42857143
MAD (Mean Absolute Deviation)		1.2244898	3.26530612	7.34693878	8.16326531	8.7755102	6.12244898	8.16326531	5.30612245	8.97959184	4.69387755	3.46938776	6.73469388	4.48979592	5.30612245	3.87755102	2.04081633

CPT – 5

Default setting/values of devices are not changed when configuring?	Complexity in structure/hardware/design/changes in the configuration	T				F			
	Improper instructions guide/ Policies	T		F		T		F	
	Lack of education/Competency and training	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	55	55	20	80	70	50	0
Respondent-B	TRUE	100	65	70	10	90	65	50	0
Respondent-C	TRUE	100	60	45	25	85	55	50	0
Respondent-D	TRUE	95	50	50	10	90	45	45	5
Respondent-E	TRUE	100	70	65	20	90	55	35	0
Respondent-F	TRUE	100	70	60	30	65	40	40	10
Respondent-G	TRUE	95	65	45	25	85	45	55	5
Respondent-H	TRUE	100	85	70	35	60	40	30	0
MEAN VALUE		98.75	65	57.5	21.88	80.63	51.88	44.38	2.5
MAD (Mean Absolute Deviation)		1.875	7.5	8.75	6.875	9.2188	9.375	7.0313	3.125

CPT – 6

System maintenance, modification and testing are not completed correctly?	Complexity in structure/hardware/design/changes in the configuration	T								F							
	Improper instructions guide/ Policies	T				F				T				F			
	Lack of education/Competency and training	T		F		T		F		T		F		T		F	
	Insufficient resources	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	95	65	55	65	60	55	40	80	75	55	50	65	65	20	0
Respondent-B	TRUE	100	85	70	60	70	50	50	35	90	70	60	50	70	60	15	0
Respondent-C	TRUE	100	85	65	55	50	55	50	45	85	70	60	55	60	60	10	0
Respondent-D	TRUE	100	95	80	75	50	35	25	25	95	80	75	70	45	30	5	1
Respondent-E	TRUE	100	95	80	70	75	70	45	30	85	85	70	65	60	50	25	5
Respondent-F	TRUE	100	90	95	80	70	55	35	25	65	65	55	45	55	45	10	0
Respondent-G	TRUE	100	95	75	65	80	65	65	20	95	85	80	75	45	50	10	5
Respondent-H	TRUE	100	95	95	85	85	70	60	45	70	50	50	45	40	35	10	0
MEAN VALUE		100	91.88	78.13	68.13	68.13	57.5	48.13	33.13	83.13	72.5	63.13	56.88	55	49.38	13.13	1.375
MAD (Mean Absolute Deviation)		0	3.9063	9.375	9.375	9.8438	8.75	9.8438	8.125	8.5938	8.75	8.9063	9.8438	8.75	9.5313	5.1563	1.8125

CPT – 7

Access control policies in computer networks are not implemented correctly?	Complexity in structure/hardware/design/changes in the configuration	T								F							
	Lack of requirements engineering/poor documentation	T				F				T				F			
	Lack of education/Competency and training	T		F		T		F		T		F		T		F	
	Insufficient resources	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	95	80	75	70	65	55	45	80	75	70	65	70	65	15	0
Respondent-B	TRUE	100	90	80	70	70	50	45	30	80	70	60	45	60	50	30	0
Respondent-C	TRUE	100	95	85	60	55	60	55	35	85	70	65	60	60	50	15	0
Respondent-D	TRUE	100	90	70	60	70	60	60	50	70	60	60	50	60	50	35	5
Respondent-E	TRUE	99	95	70	55	80	50	60	35	85	75	65	40	70	45	25	0
Respondent-F	TRUE	95	90	85	70	90	60	45	20	75	70	65	50	70	40	10	0
Respondent-G	TRUE	100	95	70	65	90	80	75	25	90	95	80	70	45	35	10	5
Respondent-H	TRUE	100	95	95	90	85	80	80	55	65	60	55	40	55	45	10	0
MEAN VALUE		99.25	93.13	79.38	68.13	76.25	63.13	59.38	36.88	78.75	71.88	65	52.5	61.25	47.5	18.75	1.25
MAD (Mean Absolute Deviation)		1.125	2.3438	7.0313	8.125	10	8.9063	9.375	9.8438	6.5625	7.3438	5	9.375	6.5625	6.25	8.4375	1.875

CPT – 8

Taking and restoration of backups are completed incorrectly?	Lack of education/Competency and training	T				F			
	Insufficient resources	T		F		T		F	
	Importance/carelessness	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	80	75	50	80	65	35	0
Respondent-B	TRUE	100	60	70	40	90	55	50	0
Respondent-C	TRUE	100	80	65	45	85	70	30	0
Respondent-D	TRUE	100	45	90	35	90	35	75	10
Respondent-E	TRUE	85	75	80	65	80	40	55	0
Respondent-F	TRUE	90	60	80	60	80	60	50	10
Respondent-G	TRUE	95	75	95	55	65	45	50	5
Respondent-H	TRUE	100	65	100	50	90	50	50	0
MEAN VALUE		96.25	67.5	81.88	50	82.5	52.5	49.38	3.125
MAD (Mean Absolute Deviation)		4.6875	10	9.8438	7.5	6.25	10	8.4375	3.9063

CPT – 9

Updates and Patches of OS, Antivirus and firmware are not managed properly?	Improper instructions guide/ Policies	T				F			
	Insufficient resources	T		F		T		F	
	Importance/carelessness	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	80	55	45	70	35	35	0
Respondent-B	TRUE	100	70	60	60	80	45	50	0
Respondent-C	TRUE	100	85	65	40	80	30	25	0
Respondent-D	TRUE	100	60	80	50	60	20	50	10
Respondent-E	TRUE	99	75	85	35	55	25	40	10
Respondent-F	TRUE	90	60	80	60	80	45	50	10
Respondent-G	TRUE	95	80	80	70	65	35	50	5
Respondent-H	TRUE	100	65	85	50	85	50	50	0
MEAN VALUE		98	71.88	73.75	51.25	71.88	35.63	43.75	4.375
MAD (Mean Absolute Deviation)		2.75	8.125	10.313	9.0625	9.375	8.2813	7.8125	4.375

CPT – 10

Supporting services or facilities not managed properly?	Lack of requirements engineering/poor documentation	T				F			
	Lack of education/Competency and training	T		F		T		F	
	Insufficient resources	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	80	65	40	55	30	30	0
Respondent-B	TRUE	100	90	70	50	60	60	50	20
Respondent-C	TRUE	100	80	60	45	60	40	35	0
Respondent-D	TRUE	95	70	85	65	40	30	55	1
Respondent-E	TRUE	100	80	70	40	70	40	60	0
Respondent-F	TRUE	70	65	80	50	70	55	35	10
Respondent-G	TRUE	95	80	95	70	65	35	50	5
Respondent-H	TRUE	100	80	80	60	55	40	40	0
MEAN VALUE		95	78.13	75.63	52.5	59.38	41.25	44.38	4.5
MAD (Mean Absolute Deviation)		6.25	5.3125	9.375	9.375	7.0313	8.125	9.375	5.375

CPT – 11

Peripheral Devices are not managed properly?	Improper instructions guide/ Policies	T				F			
	Lack of education/Competency and training	T		F		T		F	
	User ease	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	60	60	55	60	20	20	0
Respondent-B	TRUE	100	65	70	50	65	25	25	0
Respondent-C	TRUE	95	75	70	65	45	30	25	5
Respondent-D	TRUE	100	100	99	85	50	20	45	0
Respondent-E	TRUE	100	65	80	65	70	40	40	10
Respondent-F	TRUE	100	70	80	80	45	20	35	0
Respondent-G	TRUE	90	85	80	75	70	45	45	15
Respondent-H	TRUE	100	80	90	70	60	40	40	0
MEAN VALUE		98.13	75	78.63	68.13	58.13	30	34.38	3.75
MAD (Mean Absolute Deviation)		2.8125	10	8.9688	9.375	8.5938	8.75	8.2813	4.6875

CPT – 12

Strong password policy not implemented e.g. minimum password length, use of alpha-numeric and special characters?	Improper instructions guide/ Policies	T				F			
	Lack of education/Competency and training	T		F		T		F	
	User ease	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	80	90	75	40	25	10	0
Respondent-B	TRUE	100	80	60	55	60	50	45	0
Respondent-C	TRUE	100	75	85	75	35	35	35	0
Respondent-D	TRUE	100	90	70	60	70	60	40	20
Respondent-E	TRUE	90	60	80	50	65	40	30	5
Respondent-F	TRUE	100	70	80	80	30	40	25	0
Respondent-G	TRUE	90	85	80	75	70	45	45	15
Respondent-H	TRUE	100	80	90	70	60	40	40	0
MEAN VALUE		97.5	77.5	79.38	67.5	53.75	41.88	33.75	5
MAD (Mean Absolute Deviation)		3.75	6.875	7.1875	9.375	14.063	7.3438	9.0625	6.25

CPT – 13

Password is written down on paper by user incase of strong password?	Improper instructions guide/ Policies	T								F							
	Lack of education/Competency and training	T				F				T				F			
	Complexity in policy	T		F		T		F		T		F		T		F	
	Importance/carelessness	T	F	T	F	T	F	T	F	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	80	65	45	80	70	70	60	70	55	55	40	45	20	25	0
Respondent-B	TRUE	100	70	70	50	80	55	70	50	80	50	70	30	60	30	40	0
Respondent-C	TRUE	100	75	75	55	80	60	60	40	85	65	60	35	35	15	15	0
Respondent-D	TRUE	100	90	90	45	95	45	90	35	90	40	90	25	95	15	45	10
Respondent-E	TRUE	100	95	80	70	90	75	60	45	85	75	70	50	70	40	35	5
Respondent-F	TRUE	100	80	80	70	80	60	70	50	60	45	55	30	40	20	40	15
Respondent-G	TRUE	100	90	85	75	80	75	70	60	65	50	60	50	35	20	35	5
Respondent-H	TRUE	100	60	90	60	90	60	80	40	85	60	70	50	40	30	30	0
MEAN VALUE		100	80	79.38	58.75	84.38	62.5	71.25	47.5	77.5	55	66.25	38.75	52.5	23.75	33.13	4.375
MAD (Mean Absolute Deviation)		0	8.75	7.0313	10	5.4688	8.125	6.875	7.5	9.375	8.75	8.75	8.75	16.875	7.1875	7.3438	4.375

CPT – 14

Log management e.g. Proper Backup and reading of logs generated by system and devices) are not completed properly?	Lack of education/Competency and training	T				F			
	Insufficient resources	T		F		T		F	
	Importance/carelessness	T	F	T	F	T	F	T	F
Respondent-A	TRUE	100	80	80	70	55	40	30	0
Respondent-B	TRUE	100	90	90	70	70	55	40	0
Respondent-C	TRUE	100	75	75	80	60	45	25	0
Respondent-D	TRUE	100	95	100	95	50	30	30	5
Respondent-E	TRUE	100	80	90	70	75	50	20	0
Respondent-F	TRUE	100	75	80	75	60	30	25	0
Respondent-G	TRUE	95	80	95	70	65	35	45	5
Respondent-H	TRUE	100	70	100	65	85	50	40	0
MEAN VALUE		99.38	80.63	88.75	74.38	65	41.88	31.88	1.25
MAD (Mean Absolute Deviation)		1.0938	5.9375	7.8125	6.7188	8.75	8.125	7.3438	1.875

CPT – 15

Sensitive information from Technical Staff disclosed by means of social engineering?	Lack of education/Competency and training	T		F	
	Employees not satisfied	T	F	T	F
Respondent-A	TRUE	100	40	50	0
Respondent-B	TRUE	95	30	45	5
Respondent-C	TRUE	100	35	40	0
Respondent-D	TRUE	15	5	5	0
Respondent-E	TRUE	80	25	40	0
Respondent-F	TRUE	90	45	30	10
Respondent-G	TRUE	80	35	35	5
Respondent-H	TRUE	100	40	45	0
MEAN VALUE		82.5	31.88	36.25	2.5
MAD (Mean Absolute Deviation)		18.125	8.9063	9.6875	3.125

11 APPENDIX B:

11.1 Supporting Literature

Following sources were mainly approached for this purpose.

- KTH online library (ebrary).
- National Institute of Standards and Technology (NIST) Computer Security Division (CSD) publications.
- US State Computer Emergency Readiness Team's (US-CERT)
- Control System Security Program (CSSP) publications.
- Idaho National Laboratory (INL) publications.
- Center of the Protection of National Infrastructure (CPNI), UK., publications.
- Institute of Electrical and Electronics Engineers (IEEE) publications.
- National Association of State Chief Information Officers (NASCIO)
- Organisation for Economic Co-operation and Development (OECD)
- Sandia National Laboratories
- (NCS) National Communications System
- President's Information Technology Advisory Committee (PITAC)
- Networking and Information Technology Research and Development (NITRD Subcommittee)

12 APPENDIX C: BASIC DEFINITIONS

Application Server
Such server machine contains system software that triggers the server-based execution of shared business applications. Its build applications often custom built applications available to several simultaneous users.

Authentication Server
Authentication Server provides authentication services to other systems on a network.

Access Control
Access control refers to the rules and deployment mechanisms which control access to information systems, and physical access to premises. The entire subject of Information Security is based upon Access Control, without which Information Security cannot, by definition, exist.

Availability
Ensuring that information systems and the essential data are available for use as desired

Botnet
It is a collection of compromised computers that are exploited by some personage or association with no knowledge of their owners, generally for wicked purposes. Every such impure computer is cited as a bot or zombie, that's why the term zombie army is sometimes also applied as a synonym for botnet

Brute force and Dictionary Attack
Brute force and dictionary attack are often addressed together as they forced against same entities like passwords. These types of attacks can be waged against an active logon prompt or password database file [92], [71]. Bruit force attack works on hit and trail basis that is to try for the code, passwords or combination till you find the exact one. Modern computers with the distributed access and speed have made this attack successful even if the system is guarded by a strong password. All of the password can be extracted using brute attack method [92], [71], [53], [72]. In dictionary attack, attacker makes use of dictionary or database of password. These include words of English or of other language, place or proper name can also be the part of this dictionary [52], [78].

Confidentiality
Confidentiality is the concealment of information or resources

Cracker
A cracker is either a piece of software (program) whose purpose is to 'crack' the code to, say, a password; or 'cracker' refers to a person who attempts to gain unauthorized access to a computer system. Such persons are usually ill intentioned and perform malicious acts of techno-crime and vandalism

DDOS
Distributed DOS know as the denial of service attack is one of the most difficult computer generated attack to counter in which flooded computer request is generated to a specific network for some access to the service. Designing such efficient information system which can counter these scenarios is mandatory [48].

Email Servers
The purpose of email server is to store incoming mail and hand out to appropriate location it also forwards outgoing mail through the suitable channel.

FTP Server
File Transfer Protocol to exchange files over the Internet. It is used to store and share files, user can download and/or upload files remotely.

Firewall
Firewalls are security devices used to restrict access in communication networks. They prevent computer access between networks and only allow access to services which are expressly registered. They also keep logs of all activity, which may be used in investigations

Intrusion Detection Systems (IDS)
Intrusion Detection Systems are complex software applications, which monitor network activity using various techniques, such as 'intelligent agents'. Many current applications will not only detect misuse but also identify a known pattern of attack, or attack scenario. The IDS can then automatically terminate the offending session and send an alert to the Systems Administrator

Information Security Policy
IS Policy is a document that organizational contain, typically approved by higher management and circulated all over the organization to everyone with access rights to the organization's information resources.

Integrity
Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized changes.

Malware
Malware is commonly known as malicious software. Information system is infected by a malware when it is inserted into it and cause serious damages to the specific system or other systems, or to subvert them for uses other than those intended by their owners

Modem
Modulator Demodulator. A piece of communications equipment, which enables a computer to send transmissions through normal telephone lines

Man-in-the-Middle Attack
This attack occurs when a vital position that is between two communicating node is achieved by an attacker. Man-in-middle attack is of two types.

- *Sniffer attack* is the technique to sniff or copy data back and forth form the communicating stations
- *Proxy mechanism/store-and-forward mechanism* is a state of acting, to place them in line of the communication.

Data is sent by the client to other client or to the server and in either of these cases attacker acts like receiver. Attacker is undetectable to both communication parties thus able to change the stream and content of traffic. Logon identification or data is gathered by such attacks and furthermore changing the contents of message flowing. To accomplish this attack attacker changes the DNS value or the routing information, copying IP address, and defraud ARP lookups to impersonate the server from the perspective of the client and to impersonate the client from the perspective of the server

NetBIOS
NetBIOS service is a set of services that Microsoft Windows operating systems use to support network functions such as file and printer sharing

Proxy Server
Proxy Server operates as mediator connecting a workstation user and the Internet with the intention of security, administrative control, and caching service. It also acts as a gateway that split the enterprise network from the outside network.

Penetration Testing
Penetration testing is the execution of a testing plan, the sole purpose of which is to attempt to hack into a system using known tools and techniques.

Portable Storage Media
These devices are called removable media and are floppy derive, DVD/CD writer, USB/Fire wire hard derive

Routers
A device with the capacity of forward data packet's beside networks. It is used to connect at least two networks, generally two LANs or WANs or a LAN and its ISP's network.

RPC
RPC is an inter process communication technique that allows client and server software to communicate.

Spoofing Attack
Fooling system or a person is accomplished by creating misleading and false information which results in granting access or information which is not readily available. It includes **operator spoofing** which is to trick an operator resulting in providing password or an error, false location is depicted or pasteurized by the trick **location spoofing**, User normally award identification and authentication through a fabricated login screen and trick is known as **login spoofing**, **email spoofing** is to counterfeit email resulting in achieving required results and **time spoofing** is to create a bogus impression absolute or relative time [98], [51].

Spamming Attack
Spam describes the useless emails, discussion forum messages or the newsgroups which are unwanted. It can be as harmful as viruses or Trojan attached to the unrequired messages or as light as an advertisement by a vendor. Spam is an example of Denial o f Service (DoS) attack rather than a security threat. As spam increase, it becomes difficult to access or to locate rightful data. Annoying factor to the spam is consumption of internet resources (like CPU processing) hence affecting the internet performance and bandwidth availability to others. These are the floods of massages that are unwanted to the attacked email box or messaging systems [22].

Social Engineering
Attacker disguises himself and present himself to be the employee by doing this he tries to reveal information that help attacker access the system. Situation like these are described by social engineering

Setuid
It is a UNIX access rights flags that allow users to run an executable with the permissions of the executable's owner or group

SAP R/3
SAP R/3 is SAP's integrated software solution for client/server and distributed open systems. SAP's R/3 is the world's most-used standard business software for client/server computing.

SQL-Ledger
SQL-Ledger is a double entry accounting system. Accounting data is stored in an SQL Database Server and a standard web browser can be used as its user interface

Trojan
A Trojan horse is a malicious, security-breaking program that is disguised as something benign, such as a directory lister, archiver, or game. It is a type of virus which normally requires a user to perform some action before the payload can be activated

Virtual Private Network (VPN)
VPN is a network which imitate a private network, though it runs over public network lines and infrastructure. By Using specialized hardware and software, it may be constituted running over the Internet.

Web Server
A computer machine that serve up Web pages. It acknowledges HTTP requests from user through web browsers, and provides them HTTP reply in shape of web pages

Worm
A Worm is a program that propagates itself over a network, reproducing itself as it goes. The term has acquired negative connotations, as it is assumed that only crackers write worms