International Review of Management and Marketing

ISSN: 2146-4405

available at http: www.econjournals.com

International Review of Management and Marketing, 2018, 8(3), 19-25.

The Ability of Computerized Accounting Information Systems in Saudi Public Universities to Face Cyber Threats

Feras Izzat Oqlah Kasasbeh[1]*, Nawaf Samah Mohammad Thuneibat[2]

[1]Administrative Sciences Department, Community College, University of Tabuk, KSA, [2]Accounting Department, Mutah University, Jordan. *Email: fkasasbeh@ut.edu.sa/firaskasasbeh@yahoo.com

ABSTRACT

The study aimed at illustrating the history of cyber-attack experienced by Saudi Arabian organizations especially universities and overall cyber readiness. The study included 486 respondents from three different universities in Saudi Arabia. Survey was administered through printed copies of questionnaires. The data gathered were analyzed using IBM-SPSS software and AMOS plugin. Analysis revealed that participant's opinion regarding ability of the computerized accounting information system (CAIS) to face and safeguard against cyber threat depends on the awareness of the recent incidents of attack. Analysis showed that access control mediates the relationship between attack from malicious program and ability of the system to fend off those attacks. Better access control positively influences CAIS's ability to face threats. Author did not find any significant difference in people's perception across different demographic status regarding the Ability of CAIS to face cyber threat.

Keywords: Computerized Accounting Information System, Cyber-attack, Cyber Security, Cyber Readiness, Internet, Malware
JEL Classifications: M21, M4, M1

1. INTRODUCTION

Saudi Arabia has a population of 33 million with a growth rate of 2.1%. Saudi Arabia had an averaged gross domestic product of 223.63 USD Billion from 1968 until 2016. Internet was introduced in Saudi Arabia back in 1993. Although initially in 90s the access to internet was restricted and only selected staff at academic, medical, research, and government institutions had access to it, the economic development demanded expansion. In 1994, Saudi government handed over the responsibility of managing and organizing the domain. "SA" to King Abdulaziz city for Science and Technology (KACST). KACST started planning the services and policies regarding country wide deployment. 1994-1999 is considered the initial expansion period of internet in Saudi Arabia (Al-Tawil, 2001). By 1999, networks were made available commercial ISPs. Therefore, many licensed vendors were able to take part in the journey. Up to 2005, Saudi Telecommunication Company remained the prime internet service provider. Under the supervision of Saudi government they maintained and refined the access and usage policies along with regulations regarding intention to use. Policies were developed regarding illegal usage, online theft, anti-Islam activities, piracy, intrusion, injection of malware and spreading offensive propaganda. A controlling mechanism was devised that would filter both incoming and outgoing traffic. Priorities were set, and internet was made available for the educational institutions, government and business organizations first. With the passage of time the balance was achieved and public access increased (Alshahrani, 2016). A balance was achieved and contents pertaining to knowledge, education and other matters were made available to all but they were careful to ensure that these were in line with the values and teachings of Islam. Saudi Arab experienced a massive growth of internet users despite its initial limitations. The number of internet users went from 1 Lac (year 1999) to 1 million (year 2001). In 2017 that number exceeded 23 million. Nowadays, there is hardly any educational institute without internet facilities. Most of the colleges and universities offer free WIFI access to faculty and students. Universities upgraded to computerized systems for better management of work and information. However, the systems must be well protected as they handle sensitive information. Their information may be of interest to outsiders and can be stolen and used for unethical purpose. Often strong anti-malware software and internet security programs are used to protect these systems against illegal activities.

2. PROBLEM STATEMENT

To cope with the pace of development and deliver fast and accurate services many universities adopted computerized account information system (CAIS). Internet is a powerful tool for both protection and intrusion. Every year Saudi Arabia suffers from waves of cyber-attack. To safeguard valuable information from these attacks, the system needs to be upgraded regularly and ensure better access control.

3. RESEARCH SIGNIFICANCE

Technology is not without its own risks. Like every other country Saudi Arabia also is a target to cyber-attack. With the development of technology, internet has become cheaper and easily accessible to everyone. While STC have previously catered mainly to government, business and educational institutes, now almost everyone has a use for it. In recent years mischievous activities pertaining to cyber-attack from parties home and abroad have jeopardized the security of many organizations in the country. Many organizations including numerous universities fell victim to cyber-attack. Therefore, it is high time we challenged the ability of CAIS to face those threats. This study focuses on the ability of CAISs in Saudi Arabian universities to tackle cyber threats and operate effectively.

4. RESEARCH OBJECTIVES

The objectives of the research are:

1. Understanding the level of awareness of university members in Saudi Arabia regarding cyber threat and readiness.
2. Understanding the opinion of university members regarding the ability of existing computerized accounting information system (CAIS) to face cyber threat and improvement opportunities.

5. LITERATURE REVIEW

Saudi government recognizes that they need to leverage the benefits offered by internet and therefore, they emphasizes the uptake of internet technology to expedite the development in the field of education, economy, medicine, engineering and business in general. It is evident that internet is vital for more efficient government operations and delivering fast and improved services to mass people. As of today, Saudi Arabia made internet available to more than 70% of its population.

5.1. General Concept of Computerized Account Information System (CAIS)

CAIS in general deals with the direct and indirect financial activities that include transactions, data management, data processing and decision support system. The system is adopted for its easy to use user-friendly structure, fast and accurate calculating capability, easy data storage and retrieving options and summary view of the system. The system offers a decision support system to automate business process and assist decision making. CAIS implementation can begin as a simple accounting system and be expanded in to a complete enterprise resource planning with office automation, vendor-supported systems and even special purpose functions. As much as CAIS offers numerous benefits, it not always completely safe from cyber threats. Now that the technology is accessible to anyone and everyone, people/group with right skills and wrong intentions can seek for ways to penetrate into the system and steal classified information or even sabotage the system. Liang and Xue, (2009) demonstrated that this kind of intrusion can lead to severe loss of productivity and financial assets. Abu-Musa (2006) in his research on perceived cyber threats concerning CAIS mentioned organizations in Saudi Arabia and illustrated that, inability of CAIS to deal with these threats might even affect the security of the system and its stakeholders (Abu-Musa, 2006).

5.2. Cyber-attack in Saudi Arabia and Cyber Readiness

During Jubail cyber security conference, director of National Center for cyber security at KACST, Dr. Basel Alomai mentioned that the kingdom experienced 60 million cyber-attacks in 2015 alone. AlArabiya.net reported on May 2017 that, Saudi Arabia faces 164,000 cyber-attacks/per day. The hackers who are associated with these attacks, come from 120 different countries. Experts are always working to upgrade the security but, hackers are also adapting and they are changing their strategy every day. Dr. Basel mentioned that worldwide the rate of success in cyber-attack is 18% and failed attack % is roughly 26%. The rest are dealt with by the security system Hussein (2017). To avoid damage we should act proactively and invest in proactive measures rather than in reactive measures. At “Security, Information Technology 2017” workshop organized by the Ministry of Interior’s National Cyber Security Center (NCSC) in Riyadh, Kaspersky Lab mentioned that, 60% institutions in the kingdom have experienced cyber-attack over the period of last 12 months (Pierluigi Paganini-Security affairs). In that workshop, Dr. Abbad Al-Abbad (ED- strategic development and communication) emphasized on cyber readiness and nationwide infrastructure to face such threats. Earlier in 2017, Saudi Arabian Labor ministry including some other private organizations faced cyber-attack from a malware called Shamoon 2. In March 2017, a spear phishing campaign targeted government organizations of the kingdom. Attackers used weaponized word documents with macro codes designed to intrude into the systems. In August, Mamba ransomware hit Saudi Arabia. Paganini (2017). The following Figure 1 provides a cyber-readiness assessment of Saudi Arabia.

5.3. Awareness Regarding Cyber-attack in Saudi Arabian Universities

Internet was first launched as academic project at the King Fahd University of Petroleum and Minerals (KFUPM) in Dhahran in 1993 (Al-Tawil, 2001). After that KACST took the responsibility of managing the system. Therefore, universities in Saudi Arabia played important roles in the development of modern day internet technology in Saudi Arabia.

On October 2017, during the third annual cyber security workshop "Cyber Arabia," King Saud University and the Northrop Grumman Corporation announced that they are collaborating to foster innovation in cyber security among Saudi university students. "Cyber Arabia" is committed to raise awareness, deliver cyber education and arrange a cyber defence competitions across Saudi Universities (Space Watch, 2017).

The Center of Excellence in Information Assurance (CoEIA) at King Saud University (KSU) and the King Abdullah University of Science and Technology (KAUST) joined hands several times to organized workshops on awareness on cyber security. In March 2017, a workshop named "Cyber security Capacity and Capability Building: Research, Innovation and Education Perspective." Was held where teachers and senior students shared their views and commitments towards capability building to face cyber threats, Space Watch (2017) (Khan and Javed, 2016).

6. METHODOLOGY

The study aims at gathering data pertaining to people's opinion regarding the ability of the universities in Saudi Arabia to face cyber threat. The data was collected from three universities in the kingdom. Author chose not to disclose the names of the universities or participants to maintain the anonymously. The survey applied random sampling technique. The survey was administered through hard copies. 486 copies were received in return with all the necessary fields filled accordingly. Out of 486 respondents, 463 were male and 23 were female. We had 52 1st year students, 107 5th year students, 171 lecturers, 108 professors and 48 staff answering the survey questions. The number of participants from the three Universities are 178, 138 and 170. The questionnaire included 5 point Likert scale questions on likeliness of attack from various malicious programs, available anti-malware programs safeguarding the system, access control to the account information system and ability of the system to fend off those attacks. The study analyzes Ability of CAIS to face cyber-attacks considering the frequency and strength of the attack mediated by access control. Author assumes that some effect of those attacks on system's ability is accounted for by the access control to the system. An unauthorized/inexperienced/careless user may jeopardize the system's security. Therefore, access control acts as a mediator between threat from malicious programs and system's ability to fend off those attacks. Anti-malware programs installed also have some roles to play. Good antivirus and internet security software provide better protection against cyber-attack. Therefore, such security programs moderates the relations mentioned earlier.

The survey questions are designed to test the following conceptual model (Figure 2).

Author developed following hypotheses based on the conceptual model:

H_1 = Recent incidents of attack influences people's opinion regarding the ability of CAIS to face cyber threat.

H_2 = Access control mediates the relationship between attack from malicious program and ability of the system to fend off those attacks.

H_3 = There is no significant difference in people's perception across different demographic status regarding the Ability of CAIS to face cyber threat.

7. ANALYSIS AND RESULTS

Author used Statistical Package for the Social Sciences (SPSS) version 20 along with AMOS 20 plugin for data analysis and model building. The data gathered has been coded numerically and entered into SPSS. The questionnaire consists of 85 questions on four factors (showed in model) and 3 questions on demographic status of the respondents. The dependent variable "Ability of CAIS to face cyber threat" was extracted from 13 items, the independent variable "Attack from Malicious Programs" was extracted from 18 items, the mediator "Access Control" consists of 12 questionnaire items and the moderator "Anti-Malware Program" was extracted from 42 questionnaire items.

7.1. Measurement Models (A Priori Testing)

Before model building and testing the hypothesized relationships illustrated in the conceptual model, the following measurement models were tested for fitness using confirmatory factor analysis (CFA). The first model was a full measurement model considering

Figure 1: Saudi Arabia's cyber readiness (2017 cyber readiness index 2) . ©2017 cyber readiness index 2.0, all rights reserved

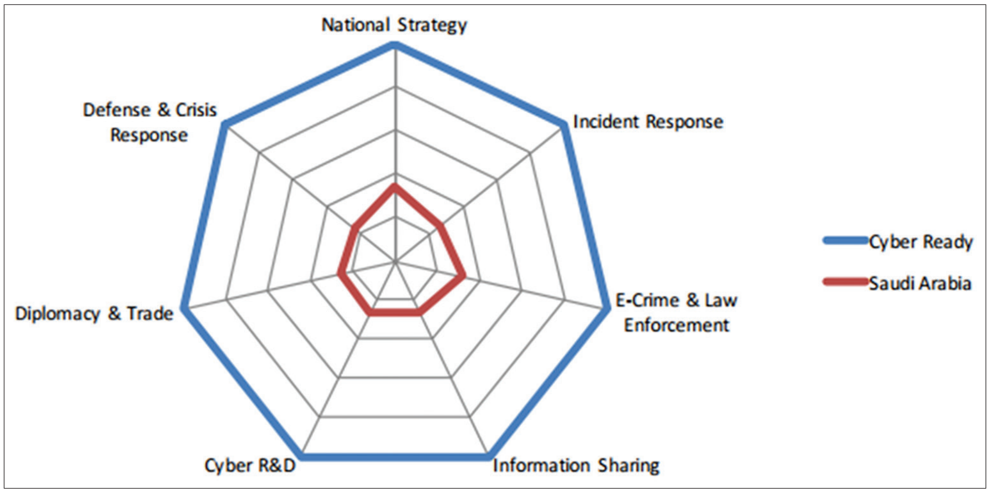
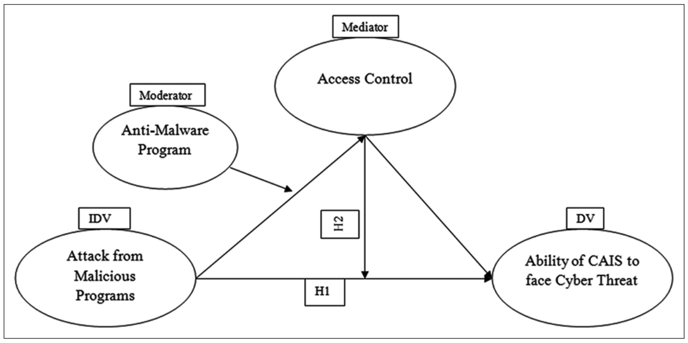


Figure 2: Conceptual model


Mediator
Access Control
Moderator
Anti-Malware Program
IDV
Attack from Malicious Programs
H2
H1
DV
Ability of CAIS to face Cyber Threat

all four individual factors. Model 1 through Model 6 illustrated alternative models where two factors were combined to form a second order construct. Model 7 illustrated a one factor model where all the factors were combined to form a second order construct. The following Table 1 shows the results obtained for each model fit indices. All the models achieved very similar results. However, the full measurement model achieved the smallest chi squared value and therefore preferred for model building.

Four factors have been extracted from the full measurement model. Table 2 shows the mean score and standard deviations associated with each variable. Table shows that, respondents tend to agree (mean score = 3.5) that attack from malicious programs is a concern for security of the computerized account information system (CAIS) in Saudi universities. Respondents shared their concerns regarding the access controls system (mean =1.3) and tend to disagree that the access control system is adequate. Respondents neither agree nor disagree on the (mean = 2.6) fact that computerized account information system (CAIS) working in Saudi Arabian universities have adequate ability to face the cyber threat. Respondents also showed concerns regarding the performance of current anti-malware programs in defeating the containing the threat (Khan and Javed, 2017). Table 2 also illustrates the correlations between the factors extracted. It shows that access control is negatively correlated with attack from malicious program (−0.283**). Therefore, better access control is likely to reduce attack (negative correlation). Better access control shows better ability to face cyber threat (.238**). Greater ability is likely to reduce attacks (−0.143**). Anti-malware is likely to provide better access control and safeguard against the intruders (0.162**).

7.2. Moderated Mediated Model

Is has been hypothesized that people's perception regarding the ability of computerized account information system (CAIS) depends on the history and fear of attack from various malicious programs. Access control to the computerized account information system (CAIS) is expected to mediate between the hypothesized dependent-independent relationships. Existence and effectiveness of anti-malware/internet security program is considered to be moderating the relationship between attack-access. Figure 3 shows the moderated-mediated model. The model was developed using AMOS version 20. After conducting CFA, four factors have been imputed for path analysis. The four factors have been entered in to the structural model and regression lines have been added as per the hypothesized relationships. Interaction factor has been calculated using SPSS and added for moderation effect. After model building the SEM model was run and achieved model fitness values were compared to the suggested baseline values. As per the stated Liang and Xue, (2009) and Abu-Musa (2006). Table 3 shows that all the model fit indices were met and therefore, the model has been considered as a good fit.

In the following Figure 4, the mediator is absent from the model. Therefore, it shows the influence of the independent variable on the dependent variable (Bollen et al., 1993). The model is a good fit and shows that the independent variable has significant influence on the dependent variable. This illustrates that people's belief on the ability of CAIS to face cyber threat depends on their past history, perception and fear of attack from Malicious programs.

Now as we have found significant IDV-DV relationship, we can analyze the effect of the mediator in Figure 3. The following Figure 5 show the step by step approach to check mediation (Baron and Kenny, 1986).

As, we see that the c` path is still insignificant but weaker, therefore, partial mediation exists (Kenny et al., 2015; Kenny and McCoach, 2003; Sarfaraz, 2017). The following Table 4 shows if there is any significant difference in participant's perception across different demographic status regarding the ability of CAIS to face cyber Threat. One way ANOVA analysis has been performed and the results have been summarized in the following Table 4. Table 4 illustrates that, for all three of the demographic factors the P values (Sig.) are >0.05. This indicates that participant's perception regarding the ability of CAIS to face cyber threat is not biased by their demographic status.

8. DISCUSSION

Cyber-attacks in Saudi Arabia are growing. Saudi Arabia is yet to achieve satisfactory level in cyber readiness. Lack of awareness has been the main culprit hence many organizations including universities were exposed to cyber-attack (http://www.citc.gov.sa). Kaspersky revealed that, Saudi Arabia is very much exposed to web threat. 40% of the organizations in the kingdom have been attacked so far. In October 2012, Saudi Oil company computer network was exposed by a virus program. Many universities were also attacked and information was exposed the same year. They were attacked with phishing mails containing malicious payload. The year later, King Saud University got attacked again and the hacker stole information on 812 users and exposed on the internet (Elnaim, 2013; M. o. C. a. I. Technology. 2015; 2016; Bragg and Rhodes-Ousley, 2004; T. C. MEA, 2015; 2016; Javed, 2018). Knowledge of these attacks and damage done makes respondents more cautious and anxious about the cyber threat. Respondents will less prior knowledge tend to undermine the situation. Hackers tend to get in to the Wifi network of the university and inject malware that would steal/wipe account information. Majority of the participants in all three universities believe that the current computerized account information system is not adequate to maintain proper access control. Moreover, employees/students sharing login credentials also jeopardize the security of the system. Use of unauthorized flash drives also creates opportunities for malware to get into the system intentionally/unintentionally.

Table 1: Comparison of measurement models

Model	χ^2	df	$\Delta\chi^2$	Δdf	CFI	GFI	NFI	RMSEA	SRMR
Full measurement model (4 factor)	3767.855	3423			0.912	0.854	0.496	0.014	0.045
Model 1 (2 factor, combines "Attack" and "Access" into one factor)	3772.073	3425	−4.218	−2	0.911	0.854	0.495	0.014	0.045
Model 2 (2 factor, combines "Attack" and "Ability" into one factor)	3777.676	3425	−9.821	−2	0.910	0.854	0.494	0.015	0.045
Model 3 (2 factor, combines "Access" and "Ability" into one factor)	3776.693	3425	−8.838	−2	0.910	0.854	0.495	0.015	0.045
Model 4 (2 factor, combines "Attack" and "Protection" into one factor)	3773.356	3424	−5.501	−1	0.910	0.854	0.495	0.015	0.045
Model 5 (2 factor, combines "Access" and "Protection" into one factor)	3774.644	3425	−6.789	−2	0.910	0.854	0.495	0.015	0.045
Model 6 (2 factor, combines "Ability" and "Protection" into one factor)	3774.651	3425	−6.796	−2	0.910	0.854	0.495	0.015	0.045
Model 7 (one factor model)	3777.286	3426	−9.431	−3	0.910	0.854	0.495	0.015	0.045

n=486, *P<0.005, **P<0.001, χ^2=Chi-square discrepancy, df=Degree of freedom, CFI: Comparative fit index, NFI: Normed fit index, RMSEA: Root mean square error of approximation. In all measurement models, error terms were free to covary one pair of items to improve fit and help reduce bias in the estimated parameter values (Reddy, 1992)

Table 2: Means, SDs and correlations

Variable	Mean±SD	1	2	3	4
Attack from Malicious programs	3.4630±0.59046	1			
Access control	1.2984±0.14117	−0.283**	1		
Ability of CAIS to face cyber threat	2.6235±0.29825	−0.143**	0.238**	1	
Anti-Malware program	2.7196±0.56482	−0.030	0.162**	−0.055	1

**Correlation is significant at the 0.01 level (2-tailed). *Correlation is significant at the 0.05 level (2-tailed). CAIS: Computerized accounting information system, SD: Standard deviation

Figure 3: Moderated-mediated model

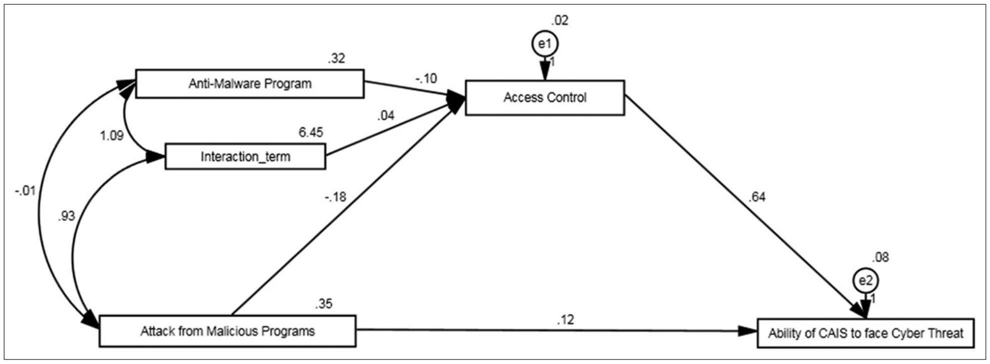
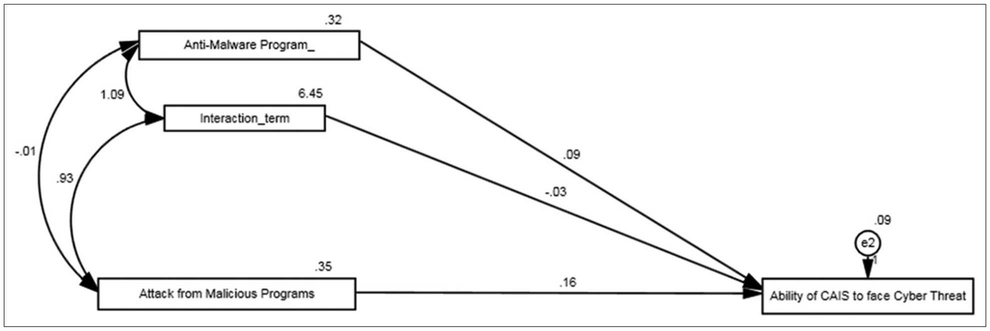


Figure 4: No mediation model



Respondents believe that the anti-malware and internet security programs in their organizations are not up to the mark when it comes to combat cyber threats. Respondents believe that proper maintenance of the system with up to date anti-malware security can provide greater chance of success against cyber threat.

The analysis illustrated that recent incidents of attack significantly influenced people's opinion regarding the ability of CAIS to face cyber threat. The kingdom has been experiencing major cyber threats since 2012. Many renowned universities including KACST, King Fahd University of Petroleum and Minerals (KFUPM), King

Table 3: SEM model fit indices

Model fit indices	Achieved values	Baseline values	Remark
χ^2	7.359	-	-
Df	2	-	-
χ^2/df	3.68	<5 “good fit,” >5 “poor fit”	Good fit
NFI	0.997	≥0.9	Good fit
RFI	0.983	≥0.9	Good fit
IFI	0.998	≥0.9	Good fit
TLI	0.988	≥0.9	Good fit
CFI	0.998	≥0.9	Good fit
GFI	0.994	≥0.9	Good fit
RMSEA	0.074	≤0.05 “close approximate fit,” >0.05 but<0.08 “marginal fit,” ≥0.10 “poor fit”	Marginal fit

*Model is a good fit [9-14]

Table 4: Perception on ability of CAIS to face cyber threat across different demographic conditions

Ability of CAIS to face cyber threat				
Demographic	n	Mean±SD	F	Significance
Gender				
Male	463	2.6246±0.29769	0.143	0.706
Female	23	2.6005±0.31531		
Role				
1st year students	52	2.6582±0.25685	0.927	0.448
5th year students	107	2.5871±0.29547		
Lecturer	171	2.6177±0.30620		
Professor	108	2.6301±0.29993		
Staff	48	2.6725±0.31382		
University				
1	178	2.6280±0.25960	1.920	0.148
2	138	2.5843±0.27451		
3	170	2.6505±0.34870		

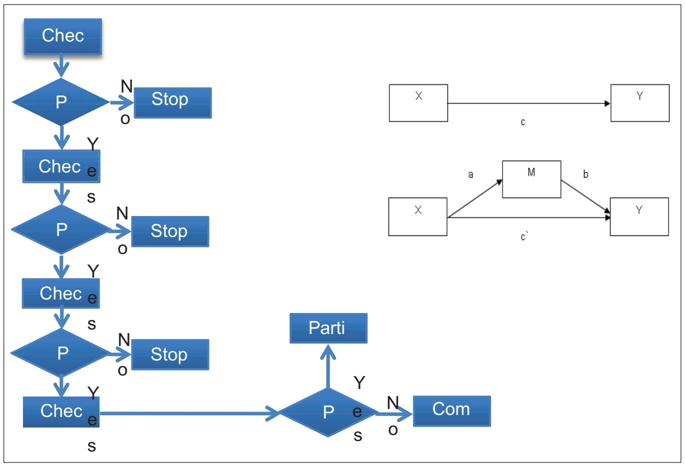
CAIS: Computerized accounting information system, SD: Standard deviation

Saud University (KSU) and the King Abdullah University of Science and Technology (KAUST) faced cyber-attacks (Kumar, 2012),. These incidents influence people’s opinion regarding CAIS’s ability to face cyber threats. Therefore, hypothesis H_1 cannot be rejected. We found that access control does indeed act as a partial mediator and influences the relationship between attack from malicious program and ability of the system to fend off those attacks. Therefore, the second hypothesis also cannot be rejected. Analysis illustrated that there is no difference in people’s perception regarding the Ability of CAIS to face cyber threat across gender, different roles or university. Therefore, hypothesis H_3 is retained.

9. CONCLUSION

The kingdom is experiencing a rapid rise of internet users, with an involvement of 70.4% of the entire population. Introduction of attractive handheld devices and social media gained massive involvement from peoples of all age, gender, social status. The use of internet along with computerized information storage and processing system goes a long way to hand in hand to deliver fast, accurate service with real time data tracking and monitoring. Many researchers put emphasis on the need for assessing the risk associated with CAIS. Their aim has been to challenge the system to improve its capability to fend off the threats associated with cyber espionage. Dhillon and Blackhouse (1996) emphasized on the conformance to rules and regulations, integrity, moral and ethical engagement to make CAIS usage a success (Fareed, 2017; Unwala, 2016). Abu-Musa (2006) conducted a study on 400 firms covering healthcare, government, oil and gas, retail, insurance, bank and manufacturing and found evidence of significant perceived threat of CAIS (Abu-Musa, 2006). Similar to this study Hanini (2012); Malami et al. (2012) worked with CAIS’s in banks and discussed risks and preventions measures (Hanini, 2012; Malami et al., 2012). Tarmidi et al. (2013) studied the CAIS threats associated with Malaysian public services (Tarmidi, 2013).

Figure 5: Mediation Baron and Kenny (2003, 2014, and 2015) approach



In this study author focused on the recent cyber-attack incidents and focused on the universities in Saudi Arabia. Internet in Saudi Arabia was introduced as a project in KACST. Since then several renowned Saudi Arabian universities have contributed in planning, managing, designing, controlling and distribution of internet across the kingdom. The CAISs functioning in the universities manage confidential business and personal information. It is of utmost importance that these information are kept safe. Cyber-attack is not new in Saudi Arabia. In fact many countries everyday fall victim to cyber-attacks. But the increasing trend of cyber-attack in Saudi Arabia is really a big concern and should be dealt with effectively.

REFERENCES

Abu-Musa, A.A. (2006), Investigating the perceived threats of computerized accounting information systems in developing countries: An empirical study on Saudi organizations. Journal of King Saud University Computer and Information Sciences, 18, 1-30.

Al-Tawil, K.M. (2001), The internet in Saudi Arabia. Telecommunications Policy, 25(8-9), 625-632.

Alshahrani, H.A. (2016), A brief history of the internet in Saudi Arabia. Tech Trends, 60(1), 19-20.

Baron, R.M., Kenny, D.A. (1986), The moderator-mediator variable distinction in social psychological research–conceptual, strategic, and statistical considerations. Journal of Personality and Social Psychology, 51(6), 1173-1182.

Bollen, K.A., Long, J.S., editors. (1993), Testing Structural Equation Models. Newbury Park, CA: Sage.

Bragg, R., Rhodes-Ousley, M. (2004), Network Security: The Complete Reference. New York: McGraw-Hill/Osborne.

Communication and Information Technology Commission. (2010), Available from: http://www.citc.gov.sa/.

Dhillon, G., Backhouse, J. (1996), Risks in the use of information technology within organizations. International Journal of Information Management, 16, 65-74.

Elnaim, B.M.E. (2013), Cyber crime in kingdom of Saudi Arabia: The threat today and the expected future. In Information and Knowledge Management, 3(1), 14-19.

Fareed, A. (2017), Saudi Facilities Sustained Nearly 1,000 Cyber-attacks in 2016, Arab News. Available from: http://www.arabnews.com/node/1061151/saudi-arabia.

Hanini, E. (2012), The risks of using computerized accounting information systems in the Jordanian banks; Their reasons and ways of prevention. European Journal of Business and Management, 4(20), 53-63.

Hussein, I.A. (2017), Available from: http://www.english.alarabiya.net/en/media/digital/2017/05/02/60-million-cyber-attacks-targeted-Saudi-Arabia-in-one-year.html. [Last accessed on 2017 May 02].

Javed, S. (2018), Does organisation behaviour affect performance of auditing firms ? International Journal of Engineering Technologiesand Management Research, 5, 90-98.

Kenny, D.A., Kaniskan, B., McCoach, D.B. (2015), The performance of RMSEA in models with small degrees of freedom. Sociological Methods and Research, 44(3), 486-507.

Kenny, D.A., McCoach, D.B. (2003), Effect of the number of variables on measures of fit in structural equation. Structural Equation Modeling, 10, 333-3511.

Khan, A., Javed, S. (2016), Determining Factors Responsible in Shifting Consumption of Mobile Data (2G to 3G). International Journal of Computer Applications, 155(14), 30-33.

Khan, A.A., Javed, S. (2017), A study of volatility behaviour of S and P BSE BANKEX return in India : A pragmatic approach using GARCH model. International Journal of Advanced and Applied Sciences, 4(4), 127-132.

Kumar, M. (2012), Saudi Arabia's King Saud University Database Hacked, Ed: The Hacker News.

Liang, H., Xue, Y. (2009), Avoidance of information technology threats: A theoretical perspective, MIS Quarterly, 33(1), 71-90.

M. o. C. a. I. Technology. (2015; 2016), 21 Million Internet users in Saudi. Available from: http://www.mcit.gov.sa/En/aboutmcit/sectordevelopment/pages/sectorindices.aspx.

Malami, A., Zaini, Z., Sherliza, P.N. (2012) Security threats of computerized banking systems (CBS): The managers' perception in Malaysia. International Journal of Economics and Finance Studies, 4(1), 21-30.

Paganini, P. (2017), 60% of Institutions in Saudi Arabia hit by Malware-based Attacks. Available from: http://www.securityaffairs.co/wordpress/63640/hacking/saudi-arabia-cyber-attacks.html.

Reddy, S.K. (1992), Effects of ignoring correlated measurement error in structural equation models. Educational and Psychological Measurement, 52(3), 549-570.

Sarfaraz, J. (2017), Journal of internet banking and commerce unified theory of acceptance and use of technology (Utaut) model-mobile banking. Journal of Internet Banking and Commerce, 22(3), 1-20. Available from: http://www.icommercecentral.com/open-access/unified-theory-of-acceptance-and-use-of-technology-utaut-modelmobile-banking.pdf.

Space Watch. (2017), Available from: https://www.spacewatchme.com/2017/10/saudi-arabia-partners-northrop-grumman-cyberarabia/.

T. C. MEA. (2015; 2016). Highest Numbers of Web Threat Incidents Reported in Qatar, UAE, Turkey and Saudi Arabia. Available from: http://www.techchannelmea.com/security/highest-numbers-webthreat-incidents-reported-qatar-uae-turkey-and-saudi-arabia.

Tarmidi, M. (2013) Computerized accounting systems threats in Malaysian public services. International Journal of Finance and Accounting, 2(2), 109-113.

Unwala, A. (2016), Cyber Security in Saudi Arabia Calls for Clear Strategies. Available from: http://www.globalriskinsights.Com/2016/07/cybersecurity-Saudi-Arabia-calls-clear-strategies/. [Last accessed on 2016 Jul 27].