Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 02, pp.65986-65994, February, 2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

# KEY FINDINGS FROM INFORMATION SECURITY SURVEY AT HIGHER EDUCATIONAL INSTITUTIONS IN THE KINGDOM OF SAUDI ARABIA

*, [1]Majedah Alkharji, [2]Hang Liu and [3]Mayyada Al Hammoshi

[1, 2]Electrical Engineering and Computer Science CUA, Washington, DC, USA
[3]School of Information Computer System, VIU, Fairfax, VA, USA

ARTICLE INFO

*Article History:*
Received 21st November, 2017
Received in revised form
20th December, 2017
Accepted 14th January, 2018
Published online 28th February, 2018

*Key words:*

Security threats,
Security systems,
Data loss,
Information leakage,
Confidentiality,
Higher educational institutions.

ABSTRACT

Advancements in technology have positively influenced the higher education in terms of delivering instructions and other services. However, as more organizations continue to embrace technology in their online operations, the risk of information security attacks cannot be underestimated. Higher education institutions have a risk of information security attacks since they have the least secure environment to protect information resources and systems. In addition, colleges, universities, and non-profit groups are very vulnerable to security breaches especially those which entail identity theft. Thus, most hackers prefer to use university and college information systems to hide their identities especially when they intend to launch attacks on commercial systems. The attackers target information systems from these institutions because they contain personal and financial information for students, alumni, employees, and other relevant stakeholders. Failure to safeguard these information systems could or have already resulted in the loss of reputation and finances of the affected individuals and institutions. A questionnaire was distributed to information technology department administrators at higher educational institutions in the Kingdom of Saudi Arabia and further analyzed. This paper aims at discussing the analysis results which include security threats that face these institutions, as well as the security systems they use.

**Citation: Majedah Alkharji, Hang Liu and Mayyada Al Hammoshi, 2018.** "Key Findings from Information Security Survey at Higher Educational Institutions in the Kingdom of Saudi Arabia", *International Journal of Current Research*, 10, (02), 65986-65994.

## INTRODUCTION

IT departments in higher educational institutions store and process confidential information about students, faculty, and alumni. There is an increase in using computer and internet-based technology which might cause information security attacks. Therefore, sensitive information such as students' records, financial information, health benefits, research information, and human resource records are at risk. Thus, they must be protected from any security incidents either from insiders and outsiders (Butler, 2013). Insiders are individuals who are authorized to access the data base and IT systems, while outsiders are individuals who have no authorization to access any essential sensitive information. Insider threats are recognized with an insider attempts to access sensitive information with no clearance or prior authorization. Most of tools and practices detect incidents after it happens. There is a lack of tools that perfectly mitigate the malicious threats by preventing the threat before their occurrence. Prevention is very important to ensure that information is very secure against anycompromise from insiders or outsiders (Cole, 2015).

This paper focuses on Saudi Arabian higher education institutions including universities and colleges. The goal of this survey is to determine the most important security problems that might happen in the academic institutions, along with the security practices and techniques they utilize to protect their information. The next section of this paper gives details about survey methodology. In the following section, the survey questions are discussed in detail. They are divided into two parts: the first part features security threats and vulnerabilities, and the second one discusses security systems and techniques. In the last section, conclusion and future works are given.

## MATERIALS AND METHODS

### Target group

The survey covered 35 different universities of central, eastern, and western regions of the Kingdom of Saudi Arabia.

**Corresponding author:* **Majedah Alkharji,**
Electrical Engineering and Computer Science CUA, Washington, DC, USA.

### Survey participants

Information technology department stakeholders included chief information security officer (CISO), IT security executive director, information security officer, information security manager, IT Security director, network security specialist, application manager, network security administrator, IT dean, application specialist, and associate dean of technical affairs.

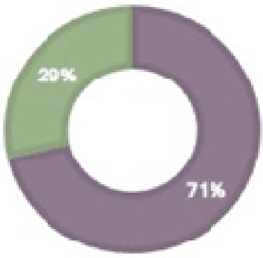

**Figure 1. Response Rate**

### Target Response Rate

There were obstacles when administering the survey include the long distance that caused difficulties when contacting the participants, lack of cooperation from members. Also, the survey was distributed during finals. Several steps were adopted to enhance the response rate and overcome those obstacles. Thus, we managed to get 25 respondents out of the 35 participants. The response rate (71%) exceeded all expectations (see Figure 1).

### Administering the Survey

The survey was conducted using Microsoft Word. Twenty-one questions were employed to measure the overall information security risk. The first nine questions encompassed information security incidents that institutions might have. The subsequent six questions measured security systems and technologies. The last six questions were about security implementations including warning systems, inspection plans, monitoring, and improvement. The survey was administered through the academic research center or IT security department of each university. Clear instructions attached with the questionnaire to explain inquiry process. Some of the questions included a comment space to provide feedback on the questions if there is any, or perhaps giving an additional view that the survey might have failed to capture.

### Survey Questions

### Security Threats and Vulnerabilities

The first two questions were crucial since they helped to specify the universities' principal security concerns (EY's Global Organization Survey 2013-2014; 2015). Figure 2shows that the top five risks threaten more than 50% of the learning institutions are malware (e.g., viruses, worms, spyware, and Trojan horses), spam, the leakage of sensitive information, account hijacking (phishing, fraud or computer abuse), and unsafe software applications. As for the second question, respondents were asked to highlight the threats that mostly concerned them the last ten years (EY's Global Organization Survey 2014). Figure 3 indicates that almost 45% of the universities agreed on having information leakage and malware at their systems. These two threats represented highest risk and infection rate.

Which threats and vulnerabilities have most increased your information security risk exposures?

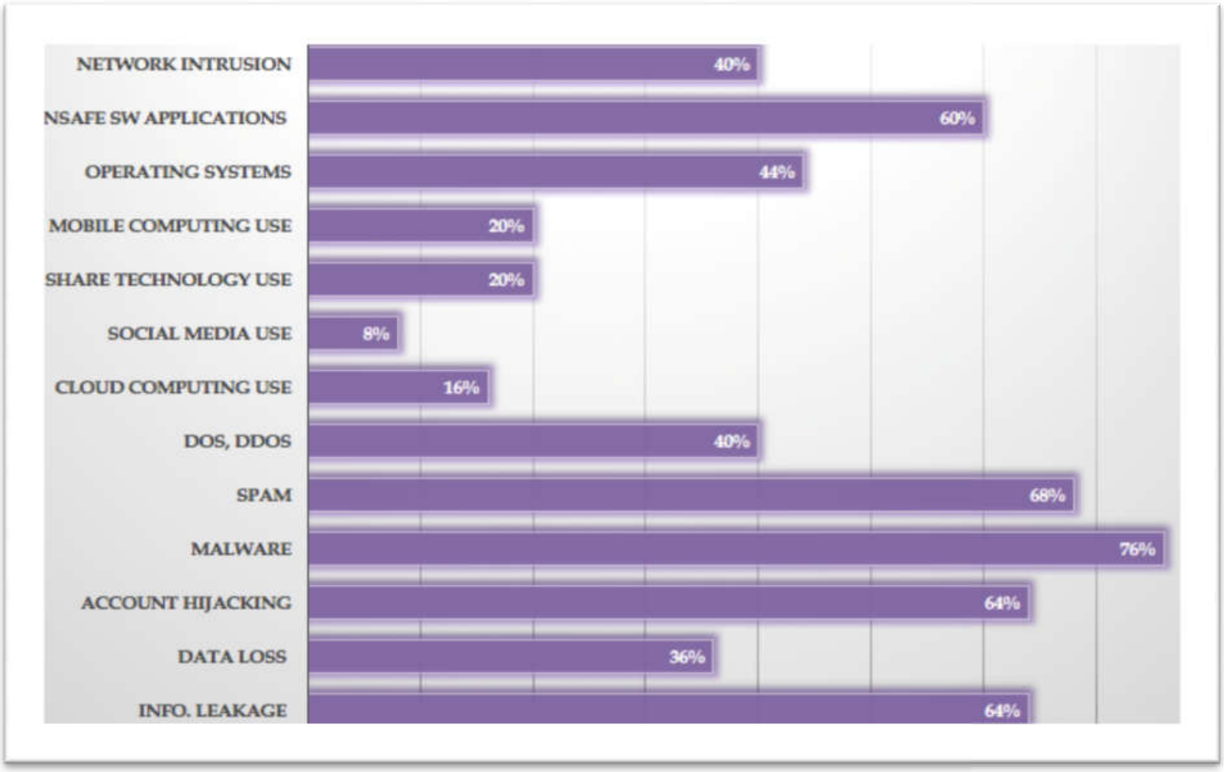

**Figure 2. Threats have most increased information security risk**

Which of those cyber threats could be the most worst issues the department had in the last ten years?

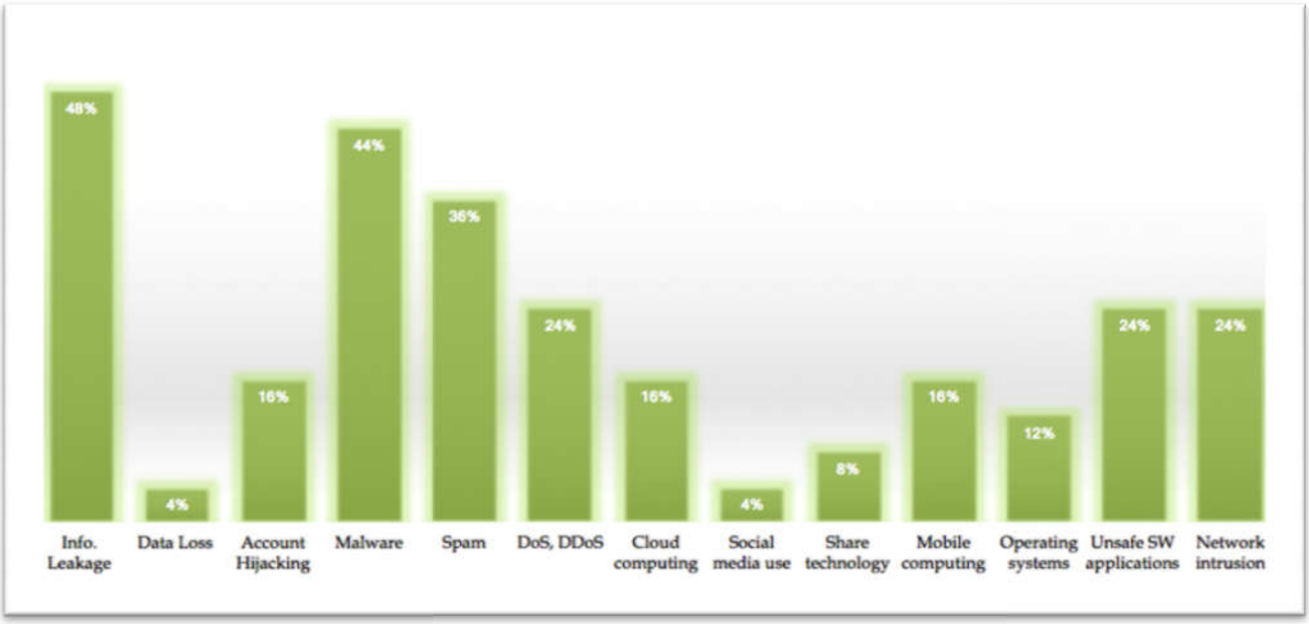

**Figure 3. Most top security threats**

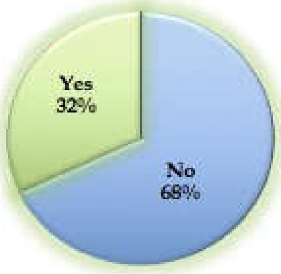

**Figure 4. Percentage of respondents who have other security concerns**

After analyzing these two answers, it has emerged that the leakage of confidential information (data breaches) needs more attention in Saudi's higher educational system.

If there are any other concerns, please specify?

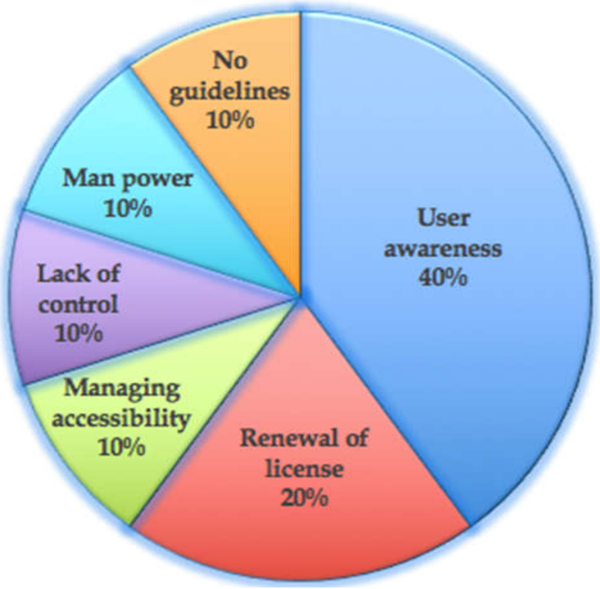

**Figure 5. Other Information Security issues**

Once information systems have been compromised, internal private documents may fall into the hands of criminals or unauthorized individuals causing confidential information leakage third of respondents highlighted other security issues (see Figure 4) like user awareness about information security risks and policies, business continuity (renewal of license for some critical applications), managing accessibility for the users, as well as the lack of control of PCs, nodes and applications. Also, respondents assured that there is an absence of guidelines for the employee to improve overall cyber security strength (Figure 5).

## Degree of Confidentiality

IT employees were asked if they have experienced an issue of information leakage. Figure 6 shows that 60% of them had this issue and they are working to improve the security measures taken. Also, they were questioned to brief us on the level of confidentiality for the sensitive information produced or handled by the departments (Risk Assessment Questionnaire 2016). Figure 7 shows that 37% of the surveyed universities assured that confidential information requires more protection against unauthorized or premature disclosure.

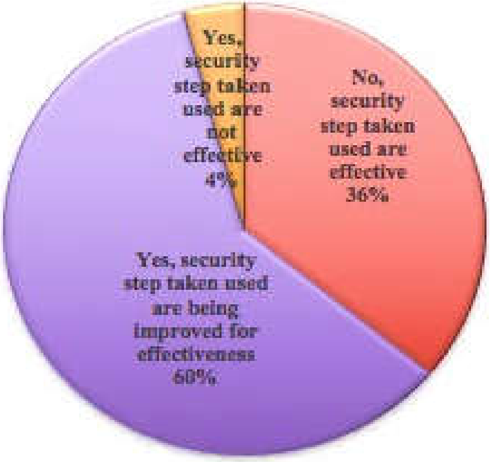

**Figure 6. Percentage of respondents who have experienced Information Leakage issue**

What is the level of confidentiality of the sensitive information?

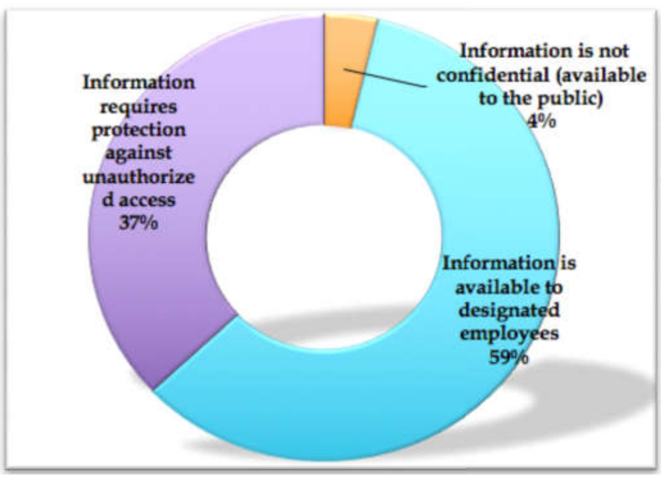

**Figure 7. Degree of Confidentiality**

### Information Leakage Reason

Participants listed the reasons that might cause the leakage of confidential documents (see Figure 8). More than 70% agreed on the top two reasons which are unauthorized access to systems or network using another person's ID, and the store and transfer confidential documents to external devices. Almost 50% of them reported that using personal emails to transfer files causes the leakage of confidential information.

What would be the reason of the data leakage?

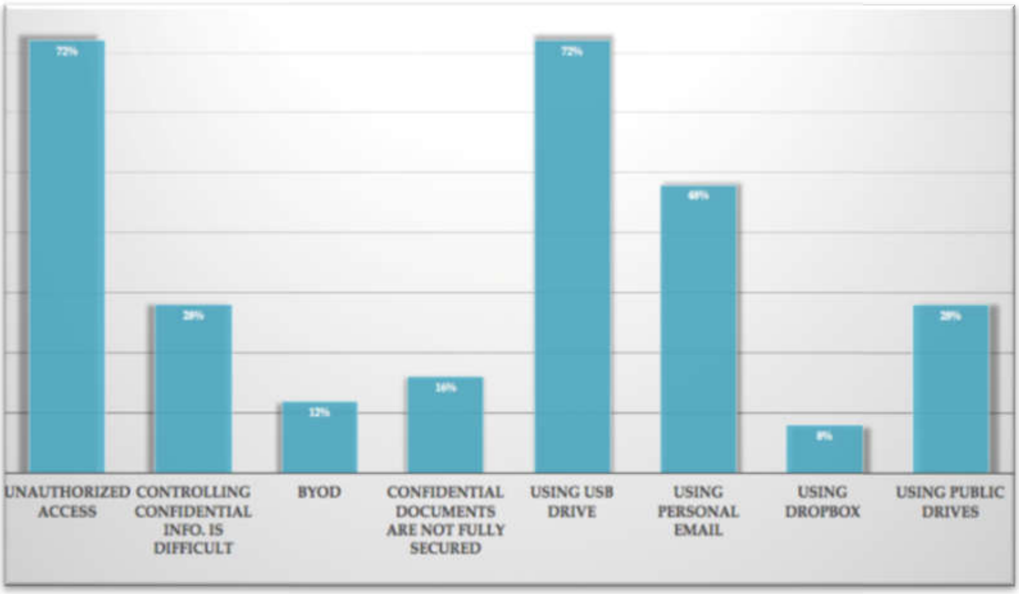

**Figure 8. Information Leakage Reasons**

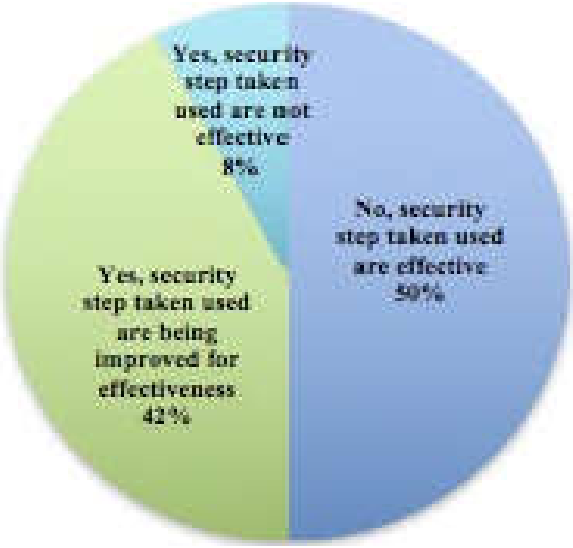

**Figure 9. Percentage of respondents who have experienced data lossissu**

### Instance of Fraud

Theft of confidential information might take place in the organization by insider or outsider hackers. Examples of fraud are diploma fraud, computer abuse, or intellectual property (Information Security Breaches Survey 2014). Fraud is considered as an important security issue faced by the educational institutions since only 34% of them were 100% secure and free from any instance of fraud, while the rest were not (Figure 11).

### Data Loss

As shown in Figure 9, half of respondents were very secured against the issue of data loss, while the other half were not. Those who have experienced data loss reported that reasons include unauthorized access, malicious software, USB drives' usage, power failure, and hardware failure (head crash) occupy the highest percentage. While fire, files or programs deletion by accident, software failure (freezing), and data corruption (system corruption, or database corruption) carry the lowest percentage (Figure 10).

### Security Systems and Operations

It's important to examine the technologies utilized to protect institutions from cyber-attacks. Security systems would help to manage the processes of security risk identification that affect the achievement of the department's objectives. Any effective technique must merge people, operations and technologies

(Cole 2015; PWC Security Survey 2013; Cyber Crime & Security Survey Report 2013). Available security solutions include people and operations, but without technologies to mitigate the risk.

Figure 13 demonstrates that almost 60% of respondents applied encryptionas a security step, while Figure 14 gives more details about the kind of encryption they use.

What would be the reason of data loss?

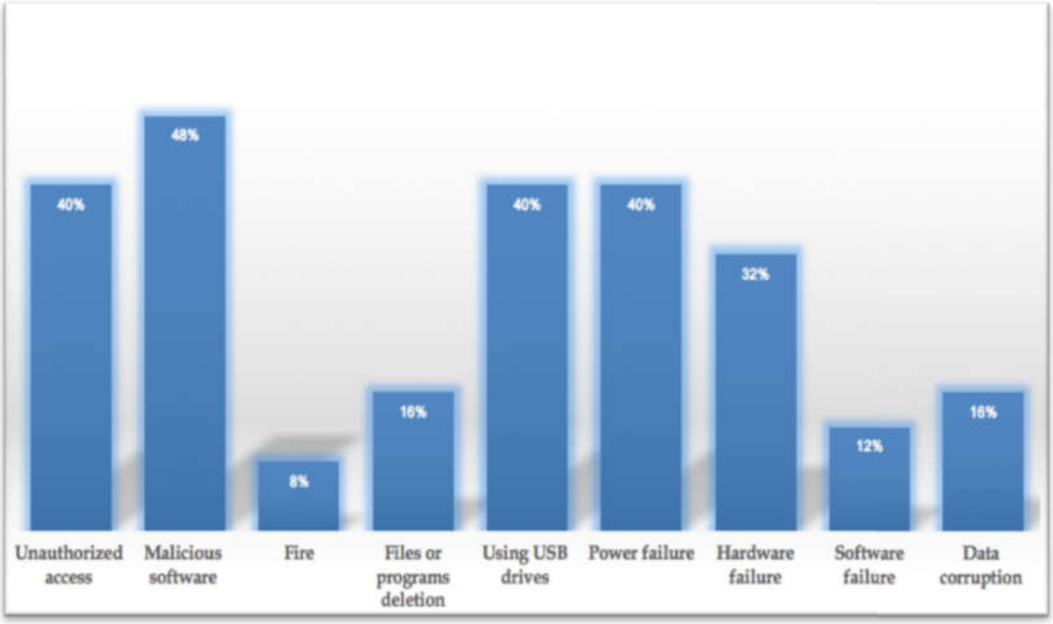

**Figure 10. Data Loss Reasons**

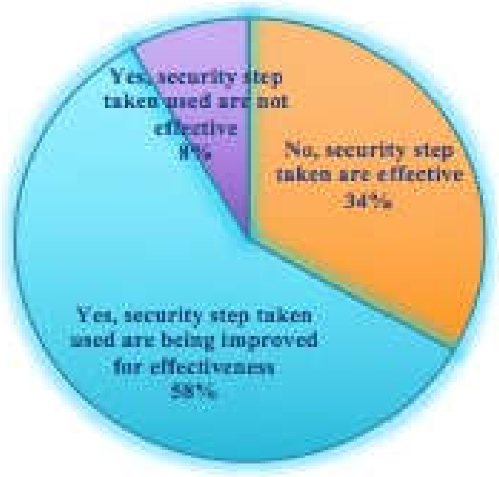

**Figure 11. Percentage of respondents who have experienced any fraud issue**

Figure 12 shows that the majority of respondents reported the use of access control, firewall, or anti-malware protection as critical security measures. Also, more than 80% of the interviewees admitted that they used network structure, or spam filters. More than 70% reported using application controls, wireless encryption, IPS (IPDS), or IDS configuration. Null practical solutions offered complete picture of security guarantee for confidential information. In addition, private individual information cannot be protected from malicious threats using the traditional security techniques like firewalls and access control. Per the answers, the respondents rarely used encryption, biometrics, authentication, and digital signature as a security step in their operation. One of the most significant concerns of higher education institutions in Saudi Arabia is that some of universities databases are not encrypted, while others employ weak algorithms as means of encryption.

Does the department have any of the following security systems or practices?

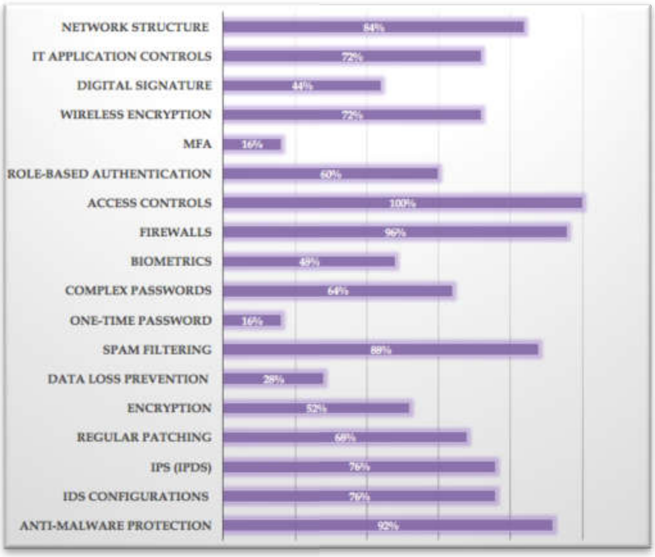

**Figure 12. Security Techniques to Identify the Information Security Risk**

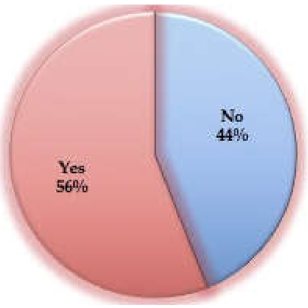

**Figure 13. Percentage of respondents**

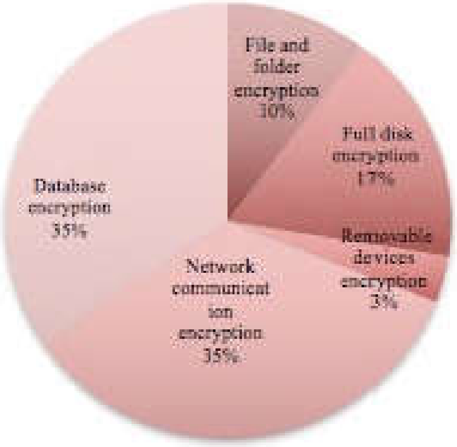

**Figure 14. Kind of Encryption they use who applied encryption**

## Desktop and Wireless Protection

Figure 15 and Figure16 explore the applied methods to protect both wireless and desktop communications (Security Survey 2016).

## Implementation Process

This part examines the implementation plan for management and technical measures. The result indicates that some surveyed institutions implement the IT security systems, standards, and policies. Also, they keep updating the latest versions of the security systems. In addition, ensure technical support from the security systems manufacturer. More details about the security implementation process is shown in Figure 17.

## Warning System

When respondents were asked about warning system or program to inspect internet connections, identify intrusion attempts, and discover the vulnerabilities, 72% had reported that they have early warning and detection system in place to mitigate the risk and reduce the chance of cyber security incidents (Figure 18). However, the majority of institutions are only able to detect uncomplicated security cases, which means that they have to get a head of cyber-attacks and develop stronger mitigation strategies to protect their systems and data (EY's Global Organization Survey 2014).

What methods does the department use to protect desktops?

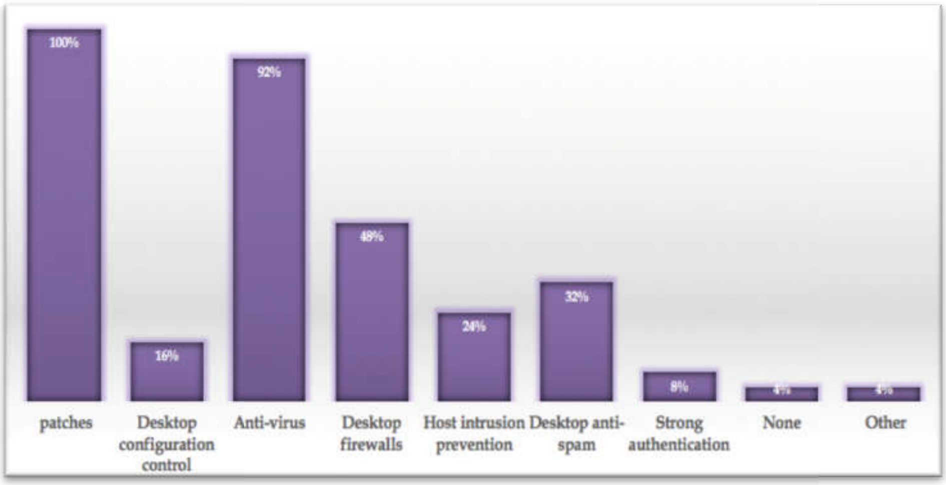

**Figure 15. Methods to protect desktop**

Which steps does your department use to secure wireless communications?

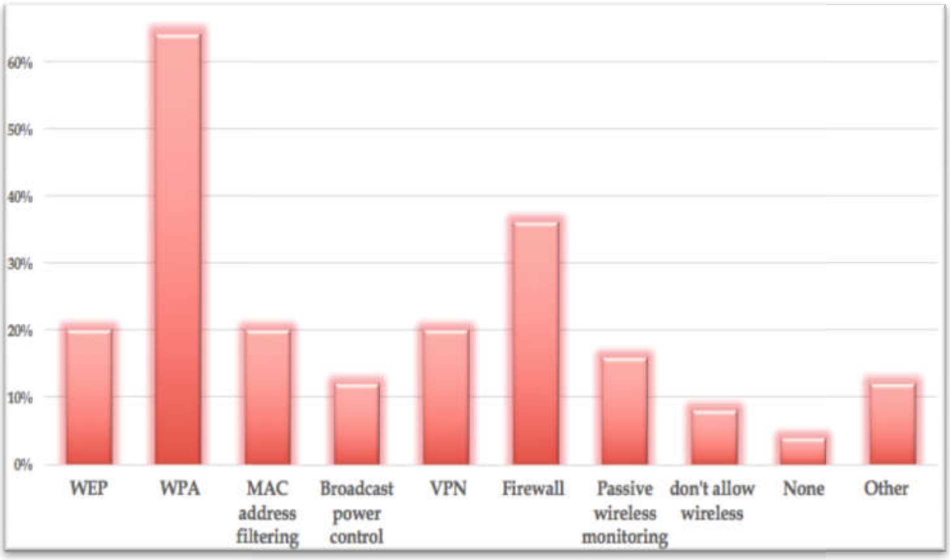

**Figure 16. Steps to secure wireless communications**

Figure 19 shows the description of waning systems installed there.

How would you describe the department security implementation process?

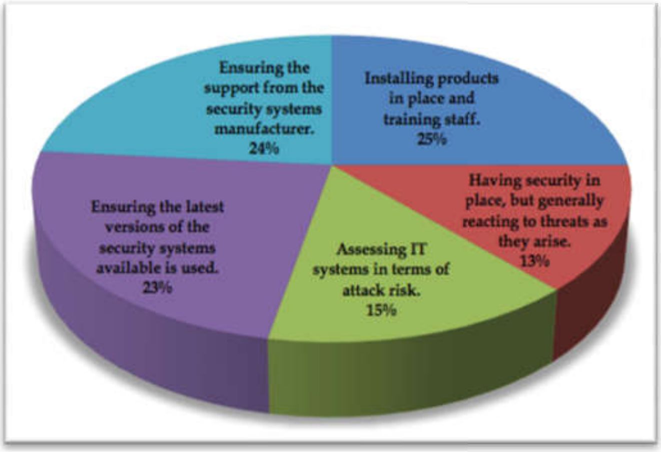

**Figure 17. Implementation process**

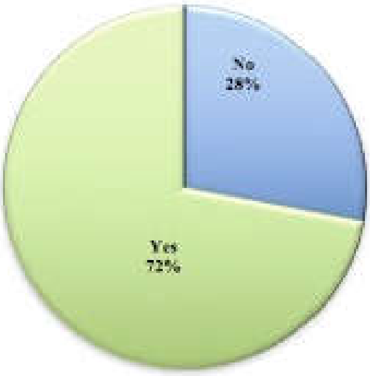

**Figure 18. Percentage of respondents who have warning system**

## Monitoring

Monitoring software is designed to monitor systems activities and help to recover from fraud and malicious activities in the potentially high information security risk areas. 48% of those institutions installed a monitoring plan (Figure 20). More details about monitoring software used is shown in Figure21.

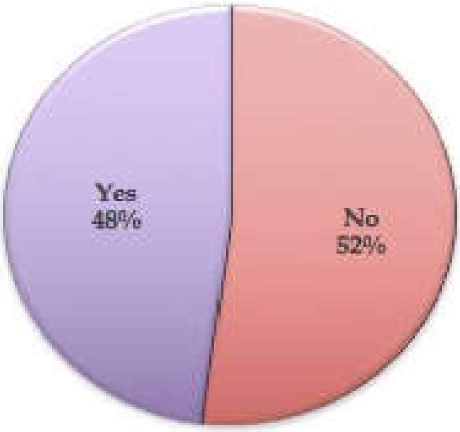

**Figure 20. Percentage of respondents who have monitoring software**

## Inspections

Inspection plans outline security policies and procedures used in reporting and responding to the cyber risks. As shown in Figure 22, percentage of those whose used inspection plans is 52%. Figure 23 gives more details about monitoring software installed there.

If yes, specify the warning systems the department installed?

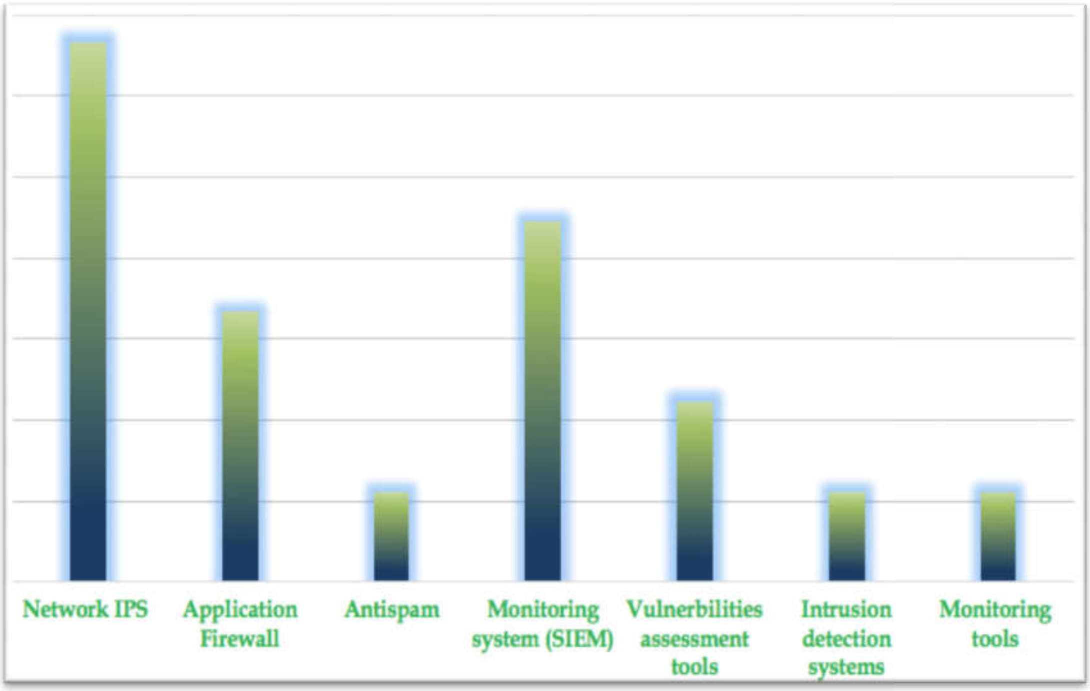

**Figure 19. Warning Systems**

If yes, specify the monitoring software the department installed?

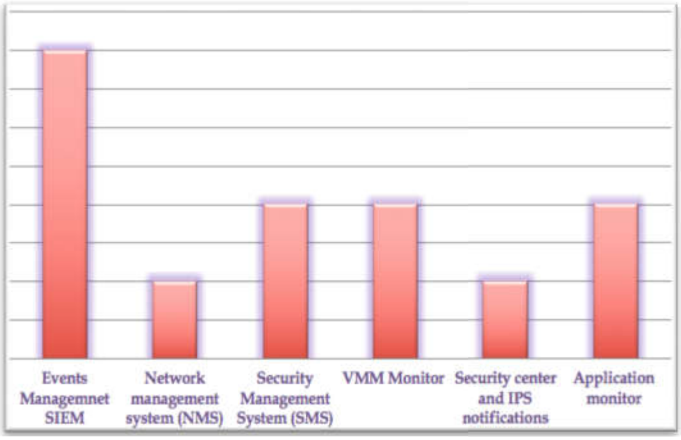

**Figure 21. Monitoring Software**

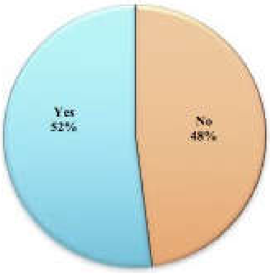

**Figure 22. Percentage of respondents who have inspection plans**

If yes, specify inspection systems the department have?

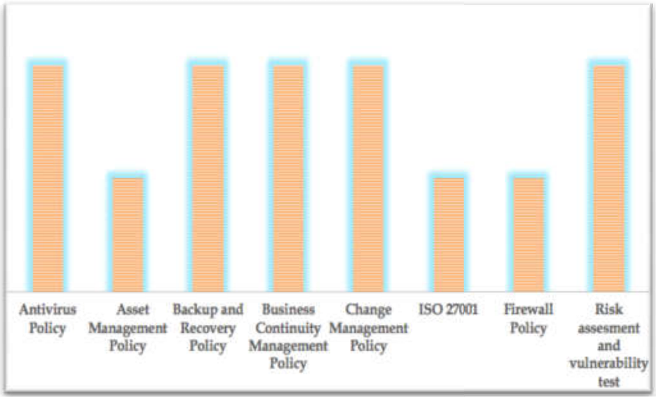

**Figure 23. Type of Inspection System**

## Incident Response Policy

Incident response addresses the damage an organization might have due to insider and outsider threats. Risk assessment plans helps to reduce the amount of damage and exposure from any threats (Cole 2015). As shown in Figure 24, only 48% of universities have an incident response plan. Figure 25 demonstrates the type of plan they installed to control the risk.

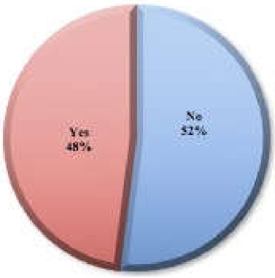

**Figure 24. Percentage of respondents who have any incident response policy**

If yes, specify the incidence response policy the department have?

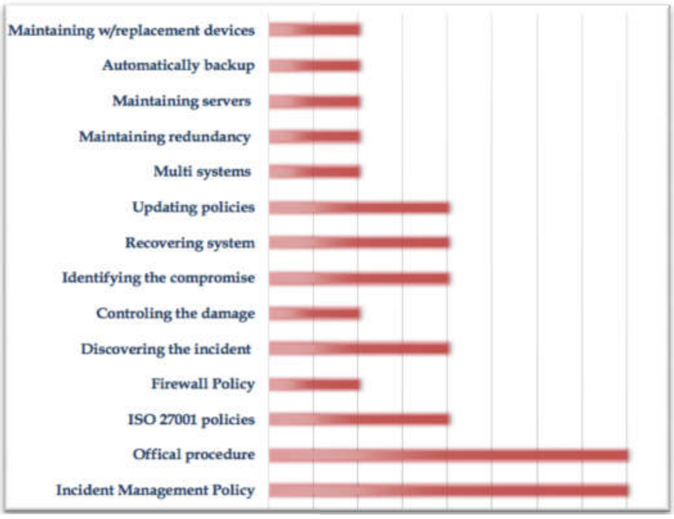

**Figure 25. Policies they follow to handle the risk**

## Improvement

The participants were questioned if the departments have any improvement methodology in place to improve the effectiveness and enhance the security systems (Cyber Crime & Security Survey Report 2013). Figure 26 shows that 44% of respondents indicated that they still need a lot to improve. Figure 27 shows the type of methodology used to improve the level of security.

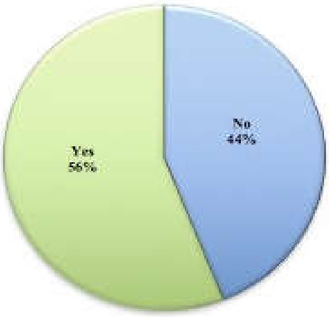

**Figure 26. Percentage of respondents who have any Improvement plans?**

If yes, specify the methodologies the department use to improve the security systems?

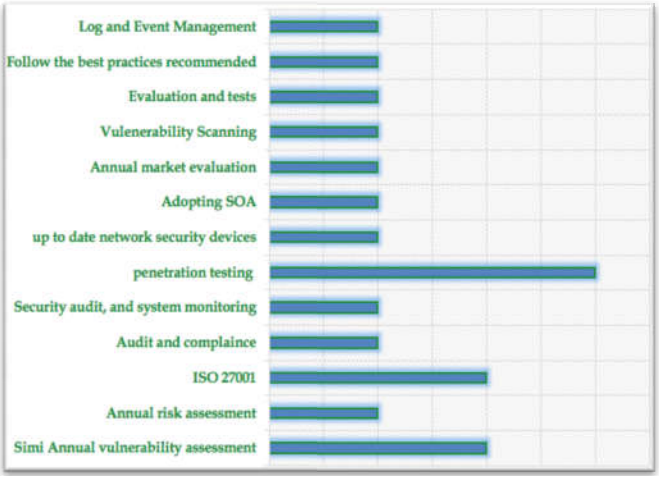

**Figure 27. Improvement plans**

### Conclusion and future work

Apparently, there is a myriad of factors that have made the higher education institutions to be at high risk of being attacked by hackers and identity theft. All organizations should take into account the importance of information security measures to curb the consequences and high costs that relate with security breaches and computer crimes. Due to the increasing rates of information security attacks, most organizations in the contemporary world have improved their level of contemplation concerning the importance of inquiring the cause of cyber-attacks as well as understanding why the organizations are exposed to such threats. Despite the fact that most information security attacks emanate from external sources, the internal attacks are more detrimental when they occur. Overall, the higher education institutions should focus more on the prevention and defense strategies. The detection of cyber threats as early as possible is one important step in mitigating the perils with the highest risk. After analyzing the survey, it is obvious that information leakage is threat with the highest risk and it needs more attention in Saudi Arabian higher educational information system. Surveyed IT employees mentioned that confidential information requires more protection against unauthorized or premature disclosure. This survey analysis provides a strong basis for future works which aims to protect universities databases from insider threats and identity thefts that could cause data breaches. A cryptographic system will be applied in cloud database server to solve the leakage of confidential information and guarantee the best security services.

### Acknowledgement

Majedah Alkharji would like to thank Ministry of Education - Saudi Arabia Culture Mission (SACM) for funding her PhD scholarship.

## REFERENCES

Butler, R. D. 2013. ‘An Examination of Issues Surrounding Information Security in California Colleges’. School of Business and Technology Management, Northcentral University. Scottsdale, Unpublished PhD Thesis.

Cole, E. 2015. ‘Insider Threats and the Need for Fast and Directed Response, A SANS Survey’, SANS Institute.

Cyber Crime & Security Survey Report, 2013. CERT Australia, Commonwealth of Australia.

EY’s Global Organization Survey 2013-2014. ‘Cyber Hacking and Information Security: Mining and Metals, EY’s Global Information Security Survey’, Ernst & Young Global Limited.

EY’s Global Organization Survey, 2014. ‘Get Ahead of Cybercrime, EY’s Global Information Security Survey’, Ernst& Young Global Limited.

EY’s Global Organization Survey, 2015. ‘Creating Trust in the Digital World, EY’s Global Information Security Survey’, Ernst & Young Global Limited.

Information Security Breaches Survey 2014. Department of Business Innovation & Skills.

PWC Security Survey 2013. ‘Key Findings from the 2013 US State of Cybercrime Survey’.

Risk Assessment Questionnaire 2016. Marquette University Risk Unit, Internal Audit, marquette.edu/riskunit/ internalaudit/documents/risk_assessment.pdf.

Security Survey 2016. Supporting Advancement/Supporting Fundraising, supportingfundraising.com.

*******