Annual ADFSL Conference on Digital Forensics, Security and Law

2008
Proceedings

Network Forensic Investigation of Internal Misuse/Crime in Saudi Arabia: A Hacking Case

Abdulrazaq Al-Murjan
Information Security Research Group, Faculty of Advanced Technology, University of Glamorgan, Pontpridd, Wales, UK, aalmurja@glam.ac.uk

Konstantinos Xynos
Information Security Research Group, Faculty of Advanced Technology, University of Glamorgan, Pontpridd, Wales, UK, kxynos@glam.ac.uk

Follow this and additional works at: https://commons.erau.edu/adfsl

Part of the Computer Engineering Commons, Computer Law Commons, Electrical and Computer Engineering Commons, Forensic Science and Technology Commons, and the Information Security Commons

Scholarly Commons Citation

Al-Murjan, Abdulrazaq and Xynos, Konstantinos, "Network Forensic Investigation of Internal Misuse/Crime in Saudi Arabia: A Hacking Case" (2016). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 1.
https://commons.erau.edu/adfsl/2008/additional-articles/1

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

(c)ADFSL

Network Forensic Investigation of Internal Misuse/Crime in Saudi Arabia: A Hacking Case

Abdulrazaq Al-Murjan
Information Security Research Group
Faculty of Advanced Technology
University of Glamorgan
Pontpridd, Wales, UK
Aalmurja@glam.ac.uk

Konstantinos Xynos
Information Security Research Group
Faculty of Advanced Technology
University of Glamorgan
Pontpridd, Wales, UK
kxynos@glam.ac.uk

ABSTRACT

There are ad-hoc guidelines and a limited policy on computer incident response that does not include computer forensic preparation procedures (e.g. logging incidents). In addition, these guidelines do not consider the requirement of Islamic law for admissible evidence at an organisational level in Saudi Arabia. Network forensic investigation might breach the Saudi law if they follow ad-hoc or international digital forensic standards such as Association of Chief Police Officers (ACPO) guidelines. This might put the organisation in a costly situation when a malicious employee sues an Islamic court. This is because the law of Saudi Arabia is complying with Islamic (Al Sharia) law. Network forensic investigators should comprehend Islamic legal requirements for admissible evidence such as privacy of a suspect, integrity and availability of evidence. These legal requirements should be translated into information technology to conduct the processes of digital forensic. These processes include searching for, collecting, preserving and presenting electronic evidence in an Islamic court. Although insider abuse/crime have not been usually reported to the law enforcement in Saudi Arabia, a hacking case is provided and examined in order to highlight shortcomings for producing e-evidence at an organisational level in Saudi Arabia. Furthermore, this case shows that there is a conflict between the technical (ad-hoc) process of collecting e-evidence which has been followed at an organisational level by network forensic investigators and the main principle of forensic procedure in Saudi Arabia. It also illustrates that there is no technical investigative standard for digital evidence. Moreover, this research addresses these issues by proposing a technical investigative standard for digital evidence. As a result of this standard, network forensic investigation is able to produce e-evidence with respect to the principles of forensic procedure in Saudi Arabia.

Keywords: Internal threats, malicious insider, network forensic investigation, hacking, formal controls for digital forensics, technical controls for digital forensics, informal controls for digital forensics, forensic procedure in Saudi Arabia

1. INTRODUCTION

Internal threats to information technology may have a significant impact on organisations (Dillon 1999; Melara and Sarriegui, 2003; Magklaras and Furnell 2004) because they usually lead to disclosure of information, modification, denial of service (DoS), illegal use, identity theft or repudiation (Gollmann 2006). These threats refer to crime/abuse when the fundamentals of an

organisation's security policy, confidentiality, integrity and availability are breached and violated by insiders. According to the British Department of Trade and Industry (DTI) in association with PriceWaterhouseCoopers who published the 'Information Security Breaches Survey 2006', malicious security incidents in organisations stemming from insiders are almost double that of those originating from unauthorised outsiders (PriceWaterHouseCoopers 2006).

Numerous attempts have been made to correctly define what a malicious insider is. According to Schneier (2000), 'a malicious insider' is defined as an employee who is an expert involved in the design of the system he is now committing an attack against. However, there are a number of internal threats that only need non-technical skills to commit a crime such as stealing the password of another user. Randazzo et al. (2005) found that 87% of internal incidents in the banking sector used simple user commands and were non-technical. Therefore, according to Schneier's definition, an employee who steals a password by looking over a colleague's shoulder at a system that she/he is unauthorised to use, and then uses this to create a threat, is not identified as an insider (Rowlingson 2005). However, Rowlingson (2005:295) defines 'an insider' as "*Someone who has skills, knowledge, resources or access, considered privileged to, or under the control of, an organisation*". This definition is broader as it also covers skills, knowledge, resources and access.

This paper accepts this definition because there are four situations that are exploited by malicious insiders to abuse or commit a crime towards the organisation's resources: these insiders are trusted, privileged to perform specific tasks, have physical access to a target system, and have knowledge of where the valuable resources are.

When an insider commits a crime or abuses a system, internal network forensic investigation should be ready to deal with internal abuse/crime such as to prove that a crime has been committed and identify the insider. It is often the case that an electronic crime has been committed and the guilty party needs to be identified. For this reason network forensic readiness is required. When internal abuse or crimes occur, digital forensic readiness is usually required in order to reveal electronic evidence (e-evidence) from networks or computers that are destined for use in court. Furthermore, Endicott-Popovsky and Frincke (2006) define network forensic readiness as "*maximizing the ability of an environment to collect credible digital evidence while minimizing the cost of an incident response"*. However, Kent and Ghavalas (2005) confirm that a large number of organisations do not have any processes or procedures in place for handling security computer events which results in mishandling admissible evidence. This is because the digital forensic practice is usually ad-hoc and lacking in widely accepted theoretical models or principles (Taylor et al. 2007).

In fact, the task of implementing a network forensic investigation is a complicated issue because it is required to comprehend the legal system. Endicott-Popovsky et al. (2007:5) believe that "*Implementing network forensic readiness in an organization will require accepting an expanded role for systems and network administrators, as well as an understanding of how legal requirements for admissible evidence can be translated into information system requirements .i.e., what network data to collect and where; what tools and procedures to use and how; who should be trained and in what topics; etc. Adopting a tool alone or a technique will not be sufficient*." It is also not an easy task because of the nature of the crime (i.e. electronic) and the evidence (i.e. digital). Electronic evidence can be exploited to hide unlawful activities. The following list provides a few of the activities:

- Anonymity
- The rapid development and variety of methods to commit a crime
- The difficulty of confirming that a crime has been committed
- Hard to find evidence
- Ability to conceal evidence

- Ease in destroying evidence (Casey 2004a; Al-Alama 2004; Technical Working Group for Electronic Crime Scene Investigation 2001)

In addition, the purpose of this research is to propose a framework of network forensic investigation at an organisational level, in order to improve the process of revealing e-evidence that is destined for use in an Islamic court. Saudi Arabia is chosen because the source of constitution of Saudi Arabia is Al Sharia law which comes from the Qur'an and Al Sunna[1]. Moreover, there is no defined way to analyse electronic crimes. A case study of an insider hacking at an organisational level, in Saudi Arabia, is analysed and examined in order to reveal the issues facing digital forensic investigators handling e-evidence. In this context, this research will address the following issues:

- How does network forensic investigation work at an organisational level in Saudi Arabia?
- What are the major problems facing network forensic investigations at an organisational level in Saudi Arabia?
- What is the proposed solution to improve the process of network forensic investigation at an organisational level in Saudi Arabia?

2. COMPUTER CRIME IN SAUDI ARABIA

800 million dollars (£400 million) have been invested by the Saudi government in the first phase of the implementation of the Country's e-Government program (Ruiz 2006*)*. The Saudi government is keen to develop a high quality of government services in order to promote an attractive environment for foreign investments (Ruiz1 2006*)*.

According to the annual report of Communication and Information Technology Commission in Saudi Arabia, the number of internet users in Saudi Arabia has increased from 1,000,000 in 2001 to 4,700,000 in 2006. It also indicates that broadband subscribers have increased from 14,000 in 2001 to 220,000 in 2006 (Communication and Information Technology Commission 2006:14). However, the government of Saudi Arabia is highly concerned about computer crimes. According to Naif Arab Academy For Security Sciences (NAASS), financial exploitation is of major concern. The cost of computer crimes in the Middle East was approximately $600,000,000 (£306,618,704) in 2000 (Al-Qasem and Al-Zhrani 2004). In the same year, the cost to Saudi companies and the public sector reached $150,000,000 (£76,655,735) (25% of the total cost of computer crime in the Middle East) (Al-Qasem and Al-Zhrani 2004).

There are a number of forms of behaviour which may lead to computer abuse/crime based on religion and public interest in Saudi Arabia. These are impersonation, espionage, information disclosure, modification, information theft, defamation adultery (false accusation of adultery), materials contradicting religion (pornography, gambling and dangerous religious ideas), forming illegal relationships by chatting via network communications, and threatening national security such as terrorist websites (Al-Sanad 2004; Mansour 2002; Al-Qasem and Al-Zhrani 2004; Al-Alma 2004). In Saudi Arabia, a survey of common cyber crimes (Alminshawi 2003) was conducted and found that the most common internet crimes were hacking, financial related offences, sexual abuse, and immoral behaviour such as obscene email, opponent websites and piracy. Importantly, the study also confirms that hacking is the highest cyber crime in the Saudi society.

In 2007, the law has been amended in Saudi Arabia to combat the growing threat of cyber-crime (IT in Saudi Arabia 2007). This law deals with offences, such as hacking or the use of internet resource to spread terrorism. This law establishes that website defacing is a crime worthy of punishment, when data theft can carry a fine of more than $130,000 or even a maximum one year prison sentence. The Saudi law has also applied this punishment to those found guilty of defamation using electronic means

[1] The Qur'an: According to Muslims, it is the speech of God.

Al Sunna: The saying and teaching of the Prophet Mohmmed.

or those who unlawfully break into private computer networks. Spreading malware could result in paying a fine of $800,000 and spending up to four years in jail, also those found guilty of distributing what is considered to be obscene martial face the same punishment. Users who create websites with pornographic content or content that defames humanity, or promotes drug use will be punished with fines of up to $1,300,000 and five years jail (IT in Saudi Arabia 2007). Table 1 shows these e-crimes with its punishments.

The Communication and Information Technology Commission in Saudi Arabia has also started the establishment of a national centre for the Saudi Arabian Computer Emergency Response Team (CERT-SA) in 2007. The team is planning to play a critical role in awareness, detection, prevention, coordination and response to information security incidents at a national level (Communication and Information Technology Commission 2006). Although this is an improvement for Saudi Arabia towards the protection of information technology, the centre is required to prove that a crime has been committed and provide the link between suspects and victims. Therefore, translating the principle of the traditional forensic investigation process in Saudi Arabia into information technology is the most important goal to be achieved.

Is the cyber crime law enough to protect information technology? Unfortunately the answer is no. E-crime presents one of the major challenges to Saudi Law enforcement and corporate security professionals because there is a lack of digital forensic readiness (Al-Qasem and Al-Zhrani 2004; Mansour 2002). Corporate security professionals in Saudi Arabia find that it is difficult to detect and prove when an e-crime has taken place and finding the link between suspects and victims. Al-Anazi (2003) confirms that most Saudi companies could not identify malicious insiders, because there is a lack of digital forensic investigation guidelines. He also confirms that detection and identification of the source of attack in the Saudi private sector was limited. Detection of the incident without identifying the source of attack was also low (Al-Anazi 2003). Section 3 will discuss the issues facing digital forensic investigation to identify the source of attack in order to improve the process of identifying a malicious insider.

Therefore, the major problem facing corporate security professionals in Saudi Arabia is a lack of network forensic readiness such as searching for, collecting and analysing e-evidence especially with respect to procedural Islamic criminal law (these procedures will be discussed in section 5).

Section	Types of Information Crime	Sanctions
Section 3	Sniffing and hijacking data and communications without permission; Blackmail; Unauthorized access to web sites in order to modify, destroy and delete data.	Prison for maximum of one year and a fine of maximum Saudi Riyals (SR) 500,000 (£73,965), or one of these sanctions.
Section 4	Computer fraud; Unauthorized access to bank account details in order to obtain data, money or services.	Prison for maximum of three years and a fine of maximum SR 2,000,000 (£295,238), or one of these sanctions.
Section 5	Unauthorized access to private data in order to sabotage or circulate it. Making the network out of services (logic bomb) Denial of Services	Prison for maximum of four years and a fine of maximum SR 3,000,000 (£443,786), or one of these sanctions.
Section 6	Materials against public interests or personal's privacy by creating, saving or sending these materials such slanders and pornography. Creating illegitimate websites in order to sell or advertise illegitimate activities (which contradict with Islam religion) such as gambling, drags and alcohols.	Prison for maximum of five years and a fine of maximum SR 3,000,000 (£443,786), or one of these sanctions.
Section 7	Creating a website for terrorist group in order to assist them to communicate, share their data or collect money and support their ides. Unauthorised physical or logical access to national security information.	Prison for maximum of ten years and a fine of maximum SR 5,000,000 (£739,644), or one of these sanctions.

Table 1. Saudi cyber-law

To address this issue, the old policy of security in organisations should be changed to accommodate the cyber crime law. Previously, organisations could only protect against cyber crime but now it is possible to bring the criminals to justice through Islamic law. The authors concluded this section by emphasising that Saudi Arabia needs forensic investigations to deal with e-crime with respect to Al-Sharia law (Al-Sanad 2004; Alminshawi 2003; Al-Qasem and Al-Zhrani 2006). Figure 1 illustrates how a malicious insider commits a crime to an organisation's resources or using these recourses to commit other crimes. This figure also demonstrates why digital forensic mishandling occurs.

The following section will illustrate a case study where network and system administrators wrongly mishandled computer evidence.

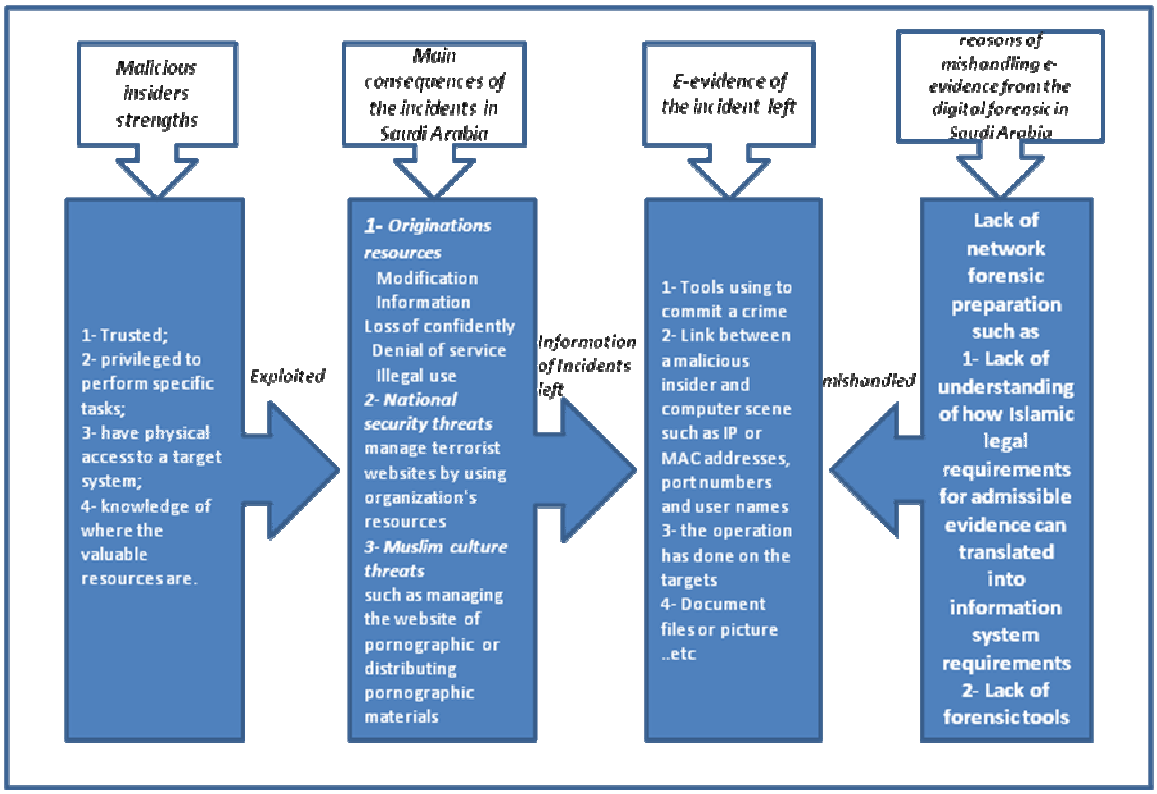

Figure 1 Main Issues of Handling E-Evidence

3. A CASE STUDY OF AN INSIDER IN SAUDI ARABIA

One of the biggest companies in Saudi Arabia has a limited policy on computer incident response that does not include computer forensic preparation procedures (e.g. logging incidents). The following case demonstrates these issues that took place, before the Saudi law of cyber crime was issued.

A malicious insider logged into the domain using the domain administrator account and illegally added his account and another account to the Internet groups (manager's groups). When the information security department detected this security incident event they disabled both accounts and the malicious insider's PC. He then used the domain administrator again and enabled both accounts and modified the configurations on his PC so that no one could access his PC. Figure 2 demonstrates the electronic evidence that a malicious insider's account was moved to open the Internet policy (will be discussed in the next section).

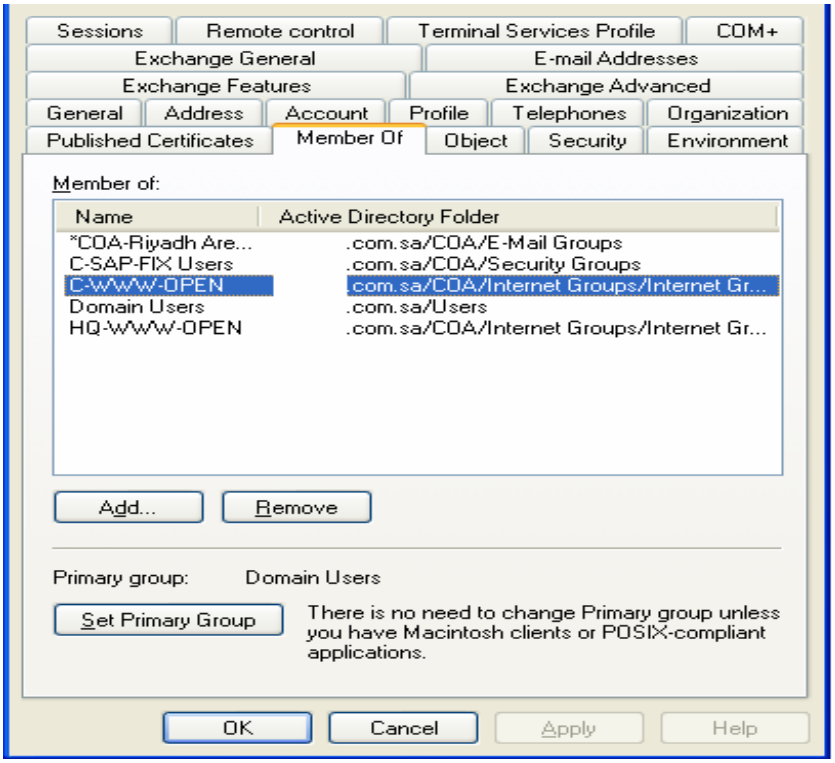

Figure 2. Evidence of Modification Internet Policy

3.1 Analyzing the Case Study

According to the law of cyber crime in Saudi Arabia, hacking is considered as illegal entry to a computerized system. Illegal entry is defined as "*an entry with a deliberate manner to the PC, a website, or information system, or network computers without being authorized*" (IT in Saudi Arabia 2007).

Two types of policies are implemented for Internet access in this organization. The first type is confined access to only one hour for normal users; whereas the second type is open (unlimited) access to the Internet for mangers and above. The insider gained unauthorized access in order to modify the policy by moving his account and another account from confined access to unlimited access.

Table 2 illustrates that there is a lack of investigative information about the malicious attack.

Network forensic readiness is required to illustrate how, when and by whom the security incident occurred, what methodology is used to attack the system, and all of this with respect to Saudi procedural criminal law. Figure 4 demonstrates a fictional attack methodology that might have been used by the insider against the system in Saudi Arabia. Therefore, network forensic readiness will play a critical role in handling computer crime evidence. This is achieved by understanding the legal requirements for admissible evidence and how that translates into information system requirements:

- What happened and how;
- What network data to collect and from where;
- What tools and procedures to use and how;

Characteristics	**Hacker case in Saudi Arabia**
Facts related to case	
Types of attack	Hacking (gaining access)
Reason of attack	To access the Internet
Facts related to network forensic investigation	
Investigator time	Not identified
Consequence	No prosecution
Evidence	Insufficient
Investigator	System and network administrators
Network forensic readiness	Ad hoc

Table 2. Information about crime and investigation

An important question has to be answered: why are corporate digital forensics investigators in Saudi Arabia not able to handle e-evidence? Research conducted by Dhillon (1999) and Melara and Sarriegui, (2003) on internal security controls provide a partial solution. Although, they examine and enhance internal security controls: formal, technical and informal, when one of the three kinds of control measures is not correctly implemented, a malicious insider poses a major risk to an organisation's resources. Therefore, the authors believe that their proposals can also be improved to examine, enhance and implement network forensic readiness at an organisational level. The following section will examine why corporate digital forensic investigators are not able to handle e-evidence. The definition of formal, technical and informal controls will be amended in order to adapt them for network forensic investigation at an organisational level.

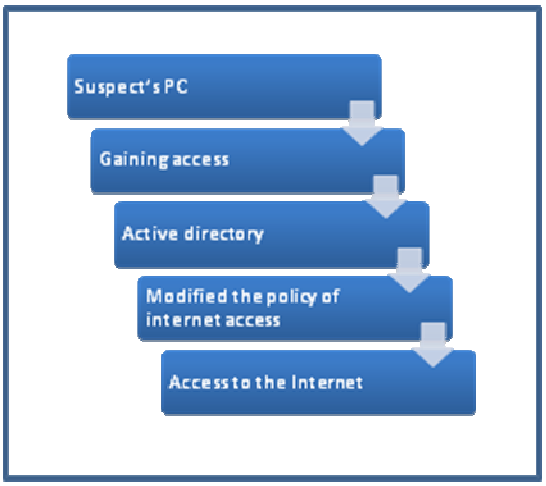

Figure 4. Attack methodology of the malicious insider against the system

3.1.1 Lack of formal controls for digital forensics

Formal controls for network forensic investigation are responsible for establishing proper policy and procedure to ensure that an organisation is able to collect and gather digital evidence, before an e-

crime takes place. Comprehension of the legal requirements for admissible evidence is required in order to translate it into information system requirements.

The majority of digital forensic investigations in Muslim countries have not understood the Islamic legal requirements for admissible evidence because their governments only recently have issued a law on combating cyber crimes. For example Saudi Arabia issued the law in 2007 and the United Arab Emirates (UAE) issued their cyber crimes law in 2006 (Gulf news report 2007). Formal controls in organisations are still not complete.

Furthermore, they do not have any processes or procedures in place for handling events that result in the requirement to produce admissible evidence (Kent and Ghavalas 2005). This is because the digital forensic practice is usually ad-hoc and lacking in widely accepted theoretical models or principles (Taylor et al. 2007). By creating guidelines on how to collect and analyse evidence and seizing hardware, it is possible to present the evidence to court. As previously mentioned, Al-Anazi (2003) confirms that in the Saudi private sector the detection and identification process of a malicious insider is limited and just detection is also very low.

Therefore, in order to identify why detection and identification of a malicious insider is limited in the majority of organisations in Saudi Arabia, the incident response policy for the case study was examined:

1. The incident policy is still under research by the information security group in the organisation and is not fully implemented yet;
2. There are no clear guidelines on:
    - How to report e-crime;
    - What data should be collected and how;
    - Where to find it;
    - What procedures to follow;
    - What tools to use to collect the evidence;
    - Who is responsible to collect the evidence;
    - How to protect the integrity of the evidence;
    - How to preserve the evidence;
    - How to protect the privacy of the suspects.
3. The policy does not consider the requirement of Saudi law (the requirement of the law will be discussed in the section 4).

Therefore, the security incident policy of this organisation is insufficient and ineffective in handling e-evidence because the translation of the Islamic legal system into information system is completely absent from this policy. The absence and misunderstanding of the legal system in the policy will lead to mishandling e-evidence. Section 4 will address this main issue by examining the principles of Al Sharia law in order to enhance formal controls.

On the other hand, the United States of America (USA) has addressed these issues and a short brief of this procedure is given. In the USA, the procedure of collecting electronic evidence from both computer networks and computer systems has been well documented in order to assist public and private forensic investigations in handling admissible electronic evidence based on the legal system of the United States (Technical Working Group for Electronic Crime Scene Investigation 2001). However, these procedures can not be implemented in Saudi Arabia, since there are differences the law. In most Western cultures publication or ownership of pornographic materials is not a crime, whereas under Al Sharia law they are a crime (Alama 2004).

The next section will look at why technical tools do not support digital forensic investigation to produce e-evidence.

3.1.2 Deficiency of technical controls for digital forensics

After the shortcomings of formal controls facing digital forensic investigation to deal with e-evidence were illustrated, the question will be answered: What is the impact of shortcomings of formal controls? What tools are missing to support digital forensic investigation? Before finding out the answer, this research will discuss in general the issues preventing digital forensic investigation from handling e-evidence.

Technical controls for network forensic investigation are tools and techniques responsible for detecting unacceptable behaviour, gathering and storing digital evidence at a technical level, such as Intrusion Detection System (IDS). There are a number of issues facing the investigation in order to collect evidence from internal threats. One of the main issues facing forensic investigations is to produce admissible evidence. From a digital forensic perspective, there is a lack of tools. The main reason for this is that tools are designed with information security in mind, rather than evidence processing (Casey 2004b). Another issue is that although network-based log files provide clues, they present a problem to investigators (Mandia et al. 2003). The logs are stored in many different formats, such as syslog and SNMP traps, and in different places each time which can cause confusion. Due to these facts, special software is required every time to access and read the logs. Therefore, these difficulties prevent digital forensic investigation from producing admissible evidence to prove an e-crime has been committed and identify a malicious insider.

Crime scene of the case study

Some information about the operating system of the organisation's network will be given in order to comprehend the shortfalls and mishandling of the case study. The organisation uses a client/server Operating System (OS). A client is an organisation user's computer which requests data or service from an organisation's server; whereas a server provides services or data to a client such as email, and directory services.

Active Directory (AD) (crime scene) is a critical database of users, computers and network resources and makes the network resources accessible to users and applications (Microsoft 2003). The groups are stored in the AD and are monitored by Microsoft Operations Manager (MOM). MOM can monitor, manage, and secure a wide range of resources including computers, applications, Web server farms, and corporate servers (MicrosoftCorporation 2005). When the insider breached the policy for accessing the Internet, MOM detected it and sent an email to the AD administrator.

From the point of digital forensic, there are a number of shortcomings in this case study and they are:

1. Audit trails were not reviewed on both sides. The aim of the audit trails is to provide a summary of information of events that can be tracked to aid in identifying events that have happened and which compromised the information systems in an organisation (Blyth and Kovacich 2006). The trails usually record a user through their identification name or number. The identification is unique and ties the user to the activities on the system (Blyth and Kovacich 2006). The audit trails will then assist network forensic investigators to identify the link between a malicious insider and the crime.
   The organisation uses a Client/server OS, therefore it is important for digital forensics to review the audit trails that are located in the security event logs on both the client and server:
   The server:
   - Audit logs: the investigators did not successfully track the logon of the administrator domain account into the AD, which would provide the link between a malicious insider and the crime;
   - Auditing policy change: the investigators missed out on a lot of evident clues that the policy was changed;

- Proxy logs: the investigators did not analyse the proxy log that proved that a malicious insider was browsing the Internet for more than the allowed period of time (i.e., one hour).

The client (a malicious insider):

- Audit logs: failure and successful events were also not examined to prove the link between a malicious insider and the crime.

2. This organisation is dependent only on one mechanism (i.e., MOM) to protect the AD;
3. A malicious insider's computer was not examined to find out the methods that were used to gain the administrator access because the investigators did not discover what tools were used by the insider.
4. The conflicting time stamps between the security incident report and the Active Directory's log. The log of the AD was only reviewed and a snapshot of the log indicates that there is a compromise of integrity. The security incident report shows the crime had taken place at 11:00 AM; whereas the AD log recorded the last logon was 11:10 AM. Figure 5 illustrates that last logon to the System was 11:10. As a result of this conflict, e-evidence is not acceptable in the court.
5. The authors interviewed corporate security professionals in the organisation and inspected the Intrusion Prevention System (IPS) and found that the IPS and IDS had not been updated for a year. Therefore, when a malicious insider used a brute force attack, the IDS could not detect it.
6. A block writer was not used to protect the integrity of the electronic evidence.

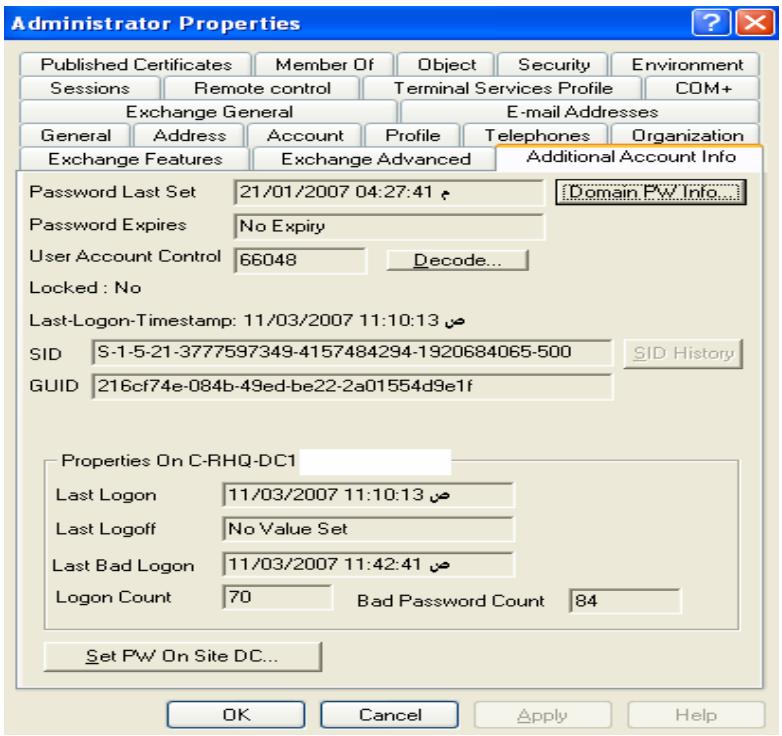

Figure 5. Evidence of the time stamp of last logon

3.1.3 Lack of informal controls for digital forensics

Informal controls are responsible for training computer forensic personnel, educating and increasing the awareness of end-users, which this is out scope of the research. In fact, there is a lack of digital

forensic experts that deal with internal threats and there are no training programmes to develop their technical skills (Alserhani 2004; Al-Sannd 2004; Al-Alama 2004; Al-Qassem and Al-Zhrani 2006). It is also vital to train end-users on how to deal with e-crime and how to report e-crime; for example by not switching a computer off when s/he has detected a crime. According to our case, it appears that the system and network administrators have no skills in handle e-evidence.

Kent and Ghavalas's (2005) propose that the addressed proactive approach naturally results in improved handling of incidents. Their paper is aimed at enhancing and improving the skills of forensic experts. Figure 6 demonstrates the malicious mechanism that was used, the shortcomings of the network forensic investigation and the reason for mishandling e-evidence in our case study.

After determining the main issues that prevent digital forensic investigation from correctly handling e-evidence, it is important for digital forensic experts to understand the Islamic legal system when handling evidence in Saudi Arabia.

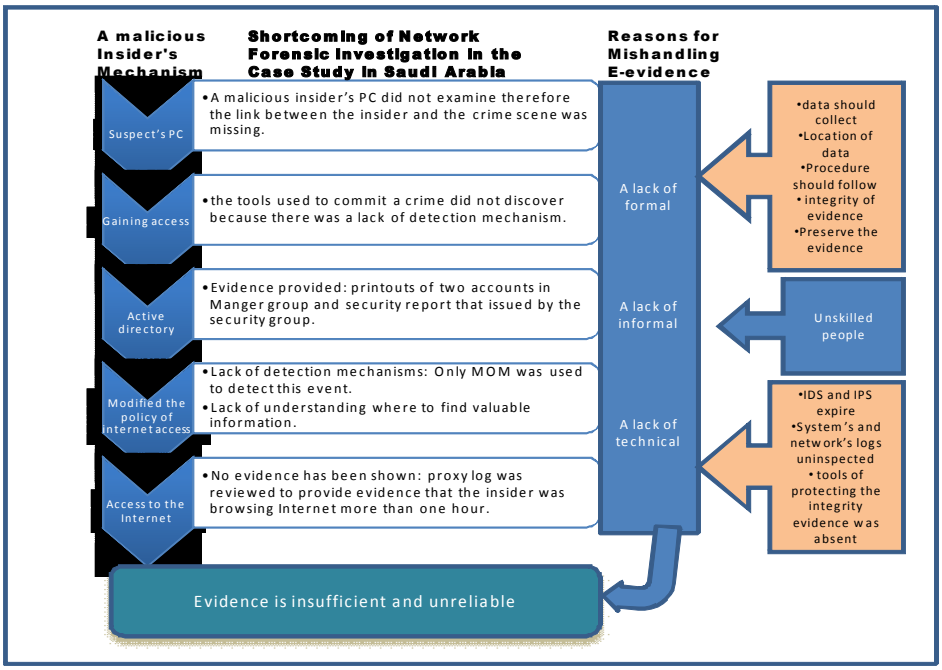

Figure 6. Major issues of mishandling evidence at the organisational level in Saudi Arabia

4. FORENSIC PROCEDURES BASED ON ISLAMIC LAW

This section will discuss the traditional forensic procedure in Saudi Arabia in order to apply it on to information systems. It will also assist the investigators in understanding the legal requirements of Islamic law in order to handle and produce e-evidence at the organisational level in Saudi Arabia.

The forensic process and procedure has been created by the country's ruler for collecting evidence, investigating and securing a verdict in order to punish the guilty based on Al Sharia law (Dafiri 2003). When a crime has taken place in a Muslim society, evidence is required to support the allegations because the Qur'an states "*bring forth your proofs, if you are truthful*." (The noble Qur'an 27:64). The aim of forensic investigations in Islam is to know the truth and achieve justice between people. This procedure includes the following steps:

4.1 Initial preparation: Inference (A stage towards proving the committing of a crime)

After a crime has been reported, the first step is to ensure the crime has been committed because the Messenger of Allah, (peace upon him) reported that "…*but evidence on the plaintiff and denied the*

right to" (Binothaimeen 2004).

Inference is defined as providing evidence based on the sources of Al Sharia law. It is also defined as providing private evidence because it is not mentioned in the Qur'an and the Sunna (Dafiri 2003). For instance, there is no process and procedure on how to collect evidence of an advanced crime such as the hacking of a system and impersonation within computers.

Nowadays, inference is called a process of collected evidence in forensic procedures. It is aimed at making sure that a crime has been committed because it is written in the Qur'an that "*If an evil-doer comes to you with a report, looks carefully into it, lest you harm a people in ignorance…*" (The Noble Qur'an 49:6).

The goal of this phase is achieved by collecting a large amount of information about a specific crime to decide whether to take forward the investigation or to close the case because of insufficient evidence.

In the Islamic law, it is important to provide the evidence when the victim reports the crime. Methods of proving crime in Al Sharia law is a controversial issue because there are two points of view (AlKarmi 2005; Al-Zohaili 1994). The first point of view believes that these methods are limited to only specific methods such as witnesses, confession and oath. These views are based on the Qur'an and the Sunna (Al-Zohaili 1994). The second point of view believes that these methods are unlimited to include any method that leads to the truth such as witness, confession, strong evidence, bearing testimony (Al Qarinah) and a scientific method.

The definition of evidence from Al-Sharia is a sign which could assist in finding an answer to a mystery (Al-Zohaili 1994). There are a number of rules for collecting evidence in Al-Sharia as follows (Al-Zohaili 1994):

- It is based on scientific techniques: evidence should not be guessed or predicted but the evidence should be extracted from a scientific process;
- It provides a link between a crime and its victim or a crime and its perpetrator. If there is a strong link between them this evidence is called strong otherwise it is weak evidence. Strong evidence is acceptable in Al-Sharia as a main method of proof in Al Sharia law; whereas weak evidence is unacceptable because it is based on prediction.

Therefore, the initial preparation is important when collecting and accumulating information about the crime that will give the investigator a clear picture; such as hearing witnesses and interviewing the victim (Dafiri 2003).

These days' computer abuses/crimes require special methods to prove and identify the offender. Searching, collecting and analysing information is required to extract the evidence in order to achieve justice.

To apply the initial preparation phase to computer abuse/crime, the proposed procedure below should be followed to ensure evidence that a crime has been committed:

- Interview the victim;
- Hear the witnesses;
- Determine the method to be used to detect and identify the incident such as IDS system, log file analysis or system administrator;
- Collect information about the operating system, file structure, types of attacks, when it happened, how, and where and the consequences of attacks (The International Association of Computer Investigative Specialists 2007);
- Determine the condition of a targeted machine (i.e., switched off or on)(ACPO 2005);
- Determine the role of the computers in a crime (e.g., a computer is a target, tool or store of evidence) (Casey 2004a);
- Record the procedure of initial preparation phase.

As previously mentioned, this phase will assist the investigator in understanding the role that the computers have in the crime. This information will be useful for the next phase because the investigator can determine what digital evidence he/she has to look for and what kind of tools. For instance, if there is a crime that involves a certain tool, the forensic investigator will look for software tools such as a Trojan Horse. Therefore, partial imaging of the drive or selective files will only be required. Initial preparation might also solve the dispute of the privacy of people because it is likely to determine the evidence before the investigation has been conducted.

4.2 Forensic investigation phase

Investigation is defined in Islam as proving the crime with admissible evidence (Dafiri 2003). Forensic investigation is a set of legal procedures that have been followed by investigators before a trial in order to discover the truth and identify the offender by inspecting and analysing the evidence of crime (Dafiri 2003). There are a number of forensic investigation processes such as:

4.2.1 Searching process

This is a process of investigation that has been conducted to search for specific evidence of a crime within private property (Dafiri 2003). The searching process is conducted only after the suspect is identified, the crime has been committed and sufficient evidence is collected. It is a technical process of finding a link between a crime and a suspect in order to prove or refute a crime.

According to article 45 of the forensic process in Saudi Arabia, an investigator has permission only to search for information and things related to a particular crime (Dafiri 2003). Therefore, the ultimate goal of this phase is to search for information that relates to the specific crime and to protect the privacy of people. In fact, the process of searching breaches Al-Sharia law because it violates the privacy of people, the Qur'an states "*spy not*" **(**The noble Qur'an 49:12**)**. However, if it is necessary, this process is allowed but it is very restricted (Al-Sannd 2004). It must be stopped immediately when evidence has been found (Dafiri, 2003).

To apply a searching process to computer abuse/crime, these steps have to be followed:

- It is vital to determine the condition of a computer whether it is switched off or on because some information might not be recovered if the computer is switched off such as volatile data (e.g., ARP cache and routing table). ACPO guidelines are useful because they refer to the condition of a computer and suggest what to do in both situations;
- The computer system should be examined physically. Documentation should include a physical description and detailed notation of any irregularities (The International Association of Computer Investigative Specialists 2007).
- A picture of the screen should be taken when it is switched on;
- To protect the integrity of the evidence, whole imaging of the offender's computer is required in the investigation of computer crime. However, it breaches the suspect's privacy, based on Islamic law. Therefore, partial file copying may solve this problem;
- It is not allowed for the forensic collector of evidence to examine the evidence because it violates the privacy of people;
- Investigation should be started where the data of evidentiary value is most likely to be found such as (The International Association of Computer Investigative Specialists 2007):
  - A full directory listing should be made to include filenames, time stamp and so forth;
  - Files created by users should be examined using file viewers such as e-mail and database;
  - Operating system files should be examined such as registry, temporary, cache and history files;
  - Only an authorised person is to analyse the evidence;
  - It is useful to examine unused and unallocated space volume for previously deleted data, deleted folders and slack space data;
- All findings should be recorded;

- All the processes should be recorded.

4.2.2 Seizing process

The main aim of the searching process is to seize the evidence for a specific crime. Seizing is retaining evidence with legal authority in order to protect the integrity and availability of evidence (Dafiri 2003). Seizing is not only to prove an allegation but is also to disprove an allegation.

The articles 55, 56, 57 and 59 in the forensic procedures in Saudi Arabian law could be applied to seize computer crime evidence (Dafiri 2003):

- It is allowed to seize the computer without accessing the data and the date and time of seizing the computer should be recorded;
- It is allowed to keep the seized contents of a computer, CDs, flash memory, floppy disks and papers away from the suspects and saved in a safe box (The International Association of Computer Investigative Specialists 2007);
- It is allowed to seize any printouts and images related to this crime;
- It is allowed for the owner to have the seized papers and documents returned;
- The investigator is responsible for protecting the confidentiality of the seized items.

4.2.3 Inspection Phase

The aim of this phase is to give the whole picture of the crime by proving the link between a crime scene and a suspect or between a suspect and a victim. This phase is important because it will prove or refute the link between a suspect, a crime and the seized items in order to provide an answer.

To apply this process to computer abuse/crime, these processes should be followed:

- The original data should not be examined in order to protect the integrity of evidence;
- The name of the suspect should be kept from the examiner to avoid lying and cronyism;
- There should be a logical order of the inspection process;
- When the contents of a seized computer are received by an examiner, the examiner should check and sign for them;
- Investigators may choose to implement a forensically sound operating system. The use of physical write-blocking hardware or software may be used in operating system environments that are not forensically sound;
- There should be one examination of the copy data;
- Examine the log files which is located in IDS, router, firewall, DHCP, and so on;
- The evidence should be extracted;
- All the processes should be recorded.

4.2.4 Expert witness

An expert witness is someone who has a high level of skill and knowledge. He has scientific knowledge of advanced methods for proving the process of linking a suspect and a crime scene. It is allowed in Islam to have an expert witness (Dafiri 2003), it is written in the Qur'an that "*So ask of those who know the Scripture if you know not*" (The noble Qur'an 16:43). There are a number of conditions when using an expert witness such as (Dafiri 2003):

- An expert is required to provide the process of linking a suspect and a crime scene;
- An expert is required to provide a report at the required time;
- An expert can have recourse to another expert;
- It is allowed for both a victim and a suspect to have recourse to a private consultant to examine the processes of the expert;
- Both a victim and a suspect can reject the report of the expert.

4.3 Reporting

The final step, digital forensic investigation is required to answer what type of crime, type of evidence, how to collect, what happened, when and who. Table 3 demonstrates the main principles of forensic procedure in Al Sharia law.

Principles of forensic procedure in Saudi Arabia	Translated into information system requirements
Chain of evidence	• Make sure a crime has taken place by reviewing the methods of detecting attacks such as IDS, IPS, users and security professionals. • What types of e-crime; • Starting to build a case from the log file of the detecting mechanism until reporting by making a link between each log based on the time stamp.
Privacy of suspect	• Make sure there is a link between a suspect and a computer crime by reviewing the network's and system's logs; • Looking for only specific information; • stop immediately when evidence has been found; • Make an image of selective files by using en-case.
Integrity of evidence	• No action is taken on the original copy; • Make an image of selective files; • Use block writing.
Availability of evidence	• Keep the evidence in safe place such as CD, flash memory and printout.

Table 3: main principles of forensic procedure in Al Sharia Law

5. CONCLUSION

The hacking case showed that organisations in Saudi Arabia are in desperate need for an investigative standard. The authors found that network forensic investigation at the organisational level uses ad-hoc guidelines to collect e-and analyse evidence. There is also a limited policy on computer incident response that does not include computer forensic preparation procedures (e.g. logging incidents). Moreover, these guidelines do not include the translation of the principle of forensic investigation process in Saudi Arabia into information systems. As a result, mishandling of e-evidence usually occurs and prevents investigators from collecting valuable evidence, based on Al Sharia law. To address these shortcomings, the chain of evidence, the privacy of the suspect, the integrity and availability of the evidence are considered in the process of network forensic investigation.

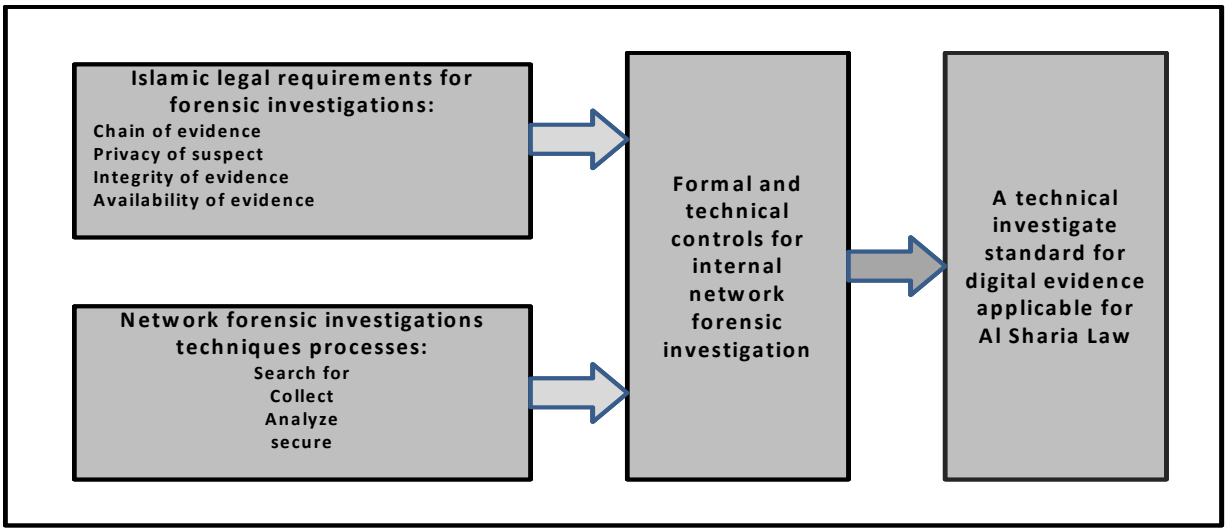

Figure 7 Proposal of technical investigative standard for digital evidence in Saudi Arabia

In the future the existing forensic procedure, in Saudi Arabia, will be enhanced with applicable digital forensic guidelines. This will then lead to an investigative standard for digital evidence. The investigative standard will include many existing computer forensic procedures in order to enhance formal and technical controls of network forensic investigation at the organisational level in Saudi Arabia. Figure 7 demonstrates the main contents of a technical investigative standard for digital evidence applicable for Al Sharia law.

REFERENCES

Al-alama, M. (2004), "Internet Crime in Islam perspective," The Arabian Journal of security studies and training, **18**(36): 5-57.

Al-Anazi, S. (2003). 'The means of the investigation in the information systems crimes'. Police Science Department. Naif Arab University for Security Sciences. Riyadh.

The Noble Qur'an in the English Language. Madinah, Saudi Arabia.

AlKarmi, A. (2005), The Wisdom Methods of AlSharia Politics, Bit Alafkar, Libnon.

Alminshawi, M. (2003). 'Internet Crimes in the Saudi Society'. Police Science Deparment. Naif Arab University for Security Sciences. Riyadh.

Al-Qasem, M. and R. Al-Zahrani (2004), "Legislations of Information Technology in Saudi Arabia: Reality, Ambitions and Obstacles." Security Research, **13**(27): 193-223.

Al-Qasem, M. and R. Al-Zahrani (2006), "A suggested National Framework for Dealing with Information Technology Crimes in Saudi Arabia," Security Research, **15**(33): 207-228.

Al-Sanad, A. (2004), The Jurisprudence of Electronic Transaction, Dar Alwarrak, Libnon.

Alserhani, M. (2004). 'Skills of Criminal Investigation in Computer and Internet Crimes'. Police Science Department. University of Naif for Security Sciences. Riyadh.

Al-Zohaili, M. (1994), The ways of proofing in Al-Sharia Law, Dar Al-Bian, Syria.

Blyth, A. and G. L. Kovacich (2006), Information Assurance, Springer, USA,.

Binothaimeen (2007), Library reading :Talk: Explain Session: Talk Third Session, http://www.ibnothaimeen.com/index.shtml, 02-08-**2007**.

Casey, E. (2004a), Digital Evidence and Computer Crime, Academic Press, California.

Casey, E. (2004b), "Network traffic as a source of evidence: tool strengths, weaknesses, and future needs." Digital Investigation**, 1**(1): 28-43.

Communication and Information Technology Commission, (2006), 'Annual Report 2006' http://www.citc.gov.sa/NR/rdonlyres/89320511-058C-4ED9-AA40-E57C4A6DB040/0/CITC_AR2007_EN.PDF, 2007.

Dafiri, S. (2003), In-Depth Studying of The Law on Criminal Procedure in Saudi Arabia, Dar Tibah, Riyadh.

Dhillon, G. (1999), "Managing and controlling computer misuse," Information Management & Computer Security, **7**(4):171-175.

Endicott-Popovsky and D. Frincke (2007), 'Embedding Forensics Capabilities into Networks', http://www.itoc.usma.edu/Workshop/2006/Program/Presentations/IAW2006-07-2.pdf, 15-10-**2007**.

Endicott-Popovsky and D. Frincke et al. (2007), "A Theoretical Framework for Organizational Network Forensic Readiness," Journal of computers, 2(3):1-11.

Furnell, S. (2004), "Enemies within: the problem of insider attacks," Computer Fraud & Security, **2004**(7): 6-11.

Gollmann, D. (2006), Computer Security, Wiley, UK.

IT in Saudi Arabia, (2008), 'The Law of Cyber Crime' http://www.itns.org.sa/Detail.asp?InSectionID=17&InNewsItemID=91, 01-01-2008.

Kent, J. and B. Ghavalas (2005). "The Unique of Collecting Corporate Evidence." Digital Investigation **2**(4): 239-243.

Magklaras, G. and S. Furnell (2004), "A preliminary model of end user sophistication for insider threat prediction in IT systems," Computers and Security, **24**(5): 371-380.

Mandia, K., C. Prosise, et al. (2003), Incident Response & Computer Forensics, Corel Ventura, U.S.A.

Mansour, A. (2002), Computer Crime from Al Sharia and Law Perspective, Dar Al Nahda, Cairo.

Melara, C. and J. Sarriegui (2003). 'A system dynamics model of an insider attack on an information system'. The 21st International Conference of the System Dynamics Society, New York, USA.

MicrosoftCorporation (2003), 2279B Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft,USA.

MicrosoftCorporation (2005). Microsoft Operations Manager 2005 Product Overview. **2007**.

PriceWaterHouseCoopers (2006). Information Security Breaches Survey 2006- Technical Report.

Randazzo, M. R., M. Keeney, et al. (2005). Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, Carnegie Mellon Software Engineering Institue**:** 1-21.

Rowlingson, R. (2005). 'Inside and out? The Information Security Threat From Insiders'. 4th European Conference on Information Warfare and Security, University of Glamorgan, UK.

Ruiz, M. (2006), 'Internet Law- Saudi Arabia Invests Billions to Improve ICTs', http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1508, 10-12-2007.

Schultz, E. E. (2002), "A Framework for Understanding and Predicting Insider Attacks," Elsevier, 21(6): 526-531.

Technical Working Group for Electronic Crime Scene Investigation (2007), 'Electronic Crime Scene Investigation: A Guide for First Responders', http://www.iwar.org.uk/ecoespionage/resources/cybercrime/ecrime-scene-investigation.pdf, 15-12-**2007**.

Taylor, C., B. Endicott-Popovsky, et al. (2007), "Specifying Digital Forensics: A Forensics Policy Approach," Digital Investigation 4(Supplement 1): 101-104.

The International Association of Computer Investigative Specialists, (2007), 'Forensic Procedure'. http://www.iacis.net/forensicprocedures, 15-12-**2007**.