Research Journal of

Business Management

ISSN 1819-1932

Academic
Journals Inc.

www.academicjournals.com

Research Journal of Business Management 8 (3): 139-156, 2014
ISSN 1819-1932 / DOI: 10.3923/rjbm.2014.139.156
© 2014 Academic Journals Inc.

Cybercrimes, Computer Forensics and their Impact in Business Climate: Bahrain Status

Adel Ismail Al-Alawi
Department of Management and Marketing, College of Business Administration, P.O. Box 32038, University of Bahrain, Bahrain

ABSTRACT

Researching on certain factors that play a vital role in the cybercrimes taking place in Bahrain. Cyber-attacks and crimes are the consequences that balance out the advantages gained from daily advancements in technologies. These attacks come in many forms. Customer awareness' is crucial to fight cybercrimes and many studies have reflected that millions of dollars are lost due to computer crimes and attacks. The conclusions of this study are based on an actual data collected from the Ministry of Interior (MOI) in Bahrain. The research findings indicate that a variety of cases being reported at the MOI. A remarkable discipline has been developed to limit and investigate computer crimes related issues: computer forensics. The Economic Impact of Cybercrimes in Business and global has been discussed. In this study computer crimes as well as computer forensics are discussed and supported by actual data from MOI and research evidences found in literatures.

Key words: Cybercrime, viruses, worms, phishing, denial of service, hacking, computer forensics, Bahrain, economic impact, computer

INTRODUCTION

The world is evolving into an ever growing state of a globalization environment. One cannot overlook the different factors affecting our daily lives as well as the future of the coming generations. Developments of new technologies are emerging into interaction methodologies between human and machines. At one end, humans are compromising some of their rights such as privacy, where at the other end technologies are serving the purpose of needs satisfaction. Yet, human nature is not predictive and easy to control. Many people are misusing technology advancements and thus hurting intentionally or not, other users. Many crimes have been conducted against cyber users. Although suggested laws and regulations have been set, these attacks are still increasing. A remarkable discipline has been developed to limit and investigate computer crimes issues: computer forensics. Computer forensics is a fairly new control scheme that centers on discovering digital verification once a computer security attack have materialized. The significant object of computer forensics is implementing a well-defined examination to discover precisely what has occurred on a digital system and who caused it.

The main purpose of this research is to present a qualitative examination of crucial issues related to auditing such as computer forensics and crimes. These issues predefine levels of vulnerability today's computer systems and networks behold. The research is divided into three key topics: Computer crimes, computer forensics and its impact in business climate in Bahrain. First, the computer attacks are introduced and discussed, followed by computer forensics related concerns

that come along with computer crimes investigations. This division will provide cyber users with a profound understanding of both topics. The reason behind choosing a qualitative overview for research is due to the lack of computer forensics cases and investigations conducted in the Kingdom of Bahrain. Although a number of cases that have been conducted, yet they are classified as confidential and their documentations and details are restricted from the public.

COMPUTER CRIMES

In general, computer crimes are basically described as criminal activities in which computers are used as tools or are targets of criminal attacks. Cyber-crimes are also defined as crimes directed against a computer, where the computer itself holds the evidences, or where the computer is used to commit the offense.

According to a study conducted by Al-Alawi and Abdelgadir (2006) "the views and opinions on the severity of various forms of computer crime may vary from one individual to another". This indicates that some people might neglect or ignore actions that others label as computer crimes. The study was basically a comparison between opinions of the society of the Kingdom of Bahrain and another study conducted in Great Britain.

Many interesting observations have been noted by Al-Alawi and Abdelgadir (2006):

- In both, the UK and the Kingdom of Bahrain a low percentage of respondents considered copying software as a crime. This is alerting because by law copying software is prohibited in both nations
- 71% of respondents believed that viruses as well as the act of "altering someone else's data" (80%), from the study conducted in the Kingdom of Bahrain, that these acts are considered as computer crimes

Figure 1 adopted from 2010/2011 Computer Security Institute 15th annual Computer Crime and Security Survey reflects the (CSI, 2011) illustrate the security technologies used to fight computer crimes. As stated, the highest percentages of respondents 97, 94.9 and 84.6% use Antivirus Software, Firewalls and Anti-Spyware Software respectively while only 43.2% uses forensic tool as a type of security technologies. This is due to the fact that the use of antivirus software, firewalls and anti-spyware software are less expensive and significantly effective when fighting attacks such as: Viruses, worms and others.

The next sections will provide an overview of different types of computer crimes. These include many types of actions. But, the main concentration of this research will be on the four most popular types of computer crimes that affect individuals as well as organization: viruses and worms, phishing, Denial of Service (DoS) and hacking.

Viruses and worms: A virus is a program that contaminates executable files. The executable file functions are altered once contaminated by a virus. The changes can occur in many forms such as the process of displaying unwanted message or the process of deleting files randomly without the user's approval. Yet, these undesired actions only take place when the executable file is run. Some viruses are harmless and entertaining to their receivers while the majority cause major damage to the registry, files, or even hardware. In contrast, worms are programs that copy themselves. The difference between a virus and a worm is that a virus is never copies itself; it is copied only when

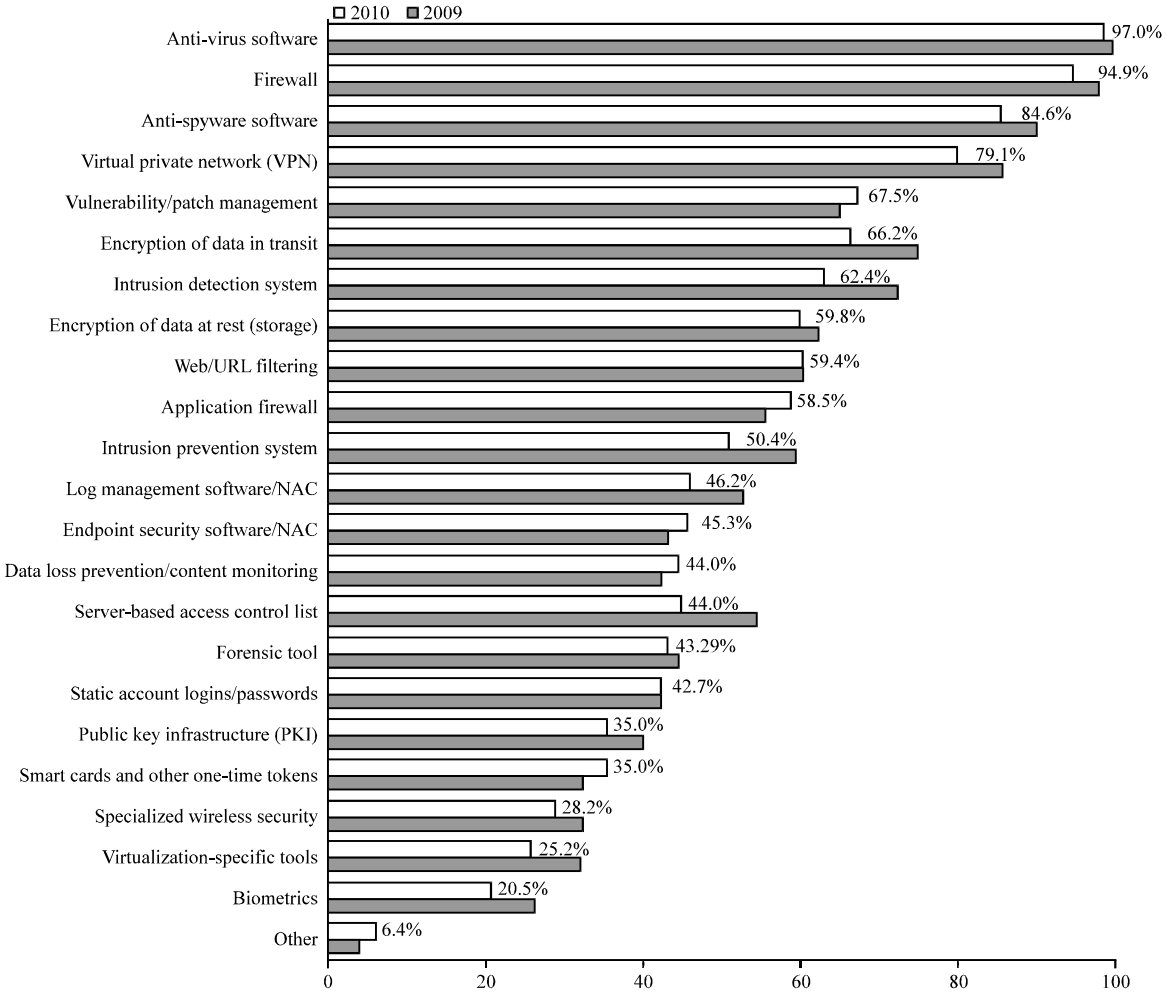

Fig. 1: Types of security technology used adopted from CSI (2011)

the executable file is run. The multiplying nature of worms causes increasing traffic on the Internet or network used. Some types of worms hold viruses as well, this causes twice the damage as a single worm would cause.

Phishing: There is a variety of intrusion approaches that offenders have developed to commit cybercrimes. Some approaches used include conducting researches in order to attack a selective portion of the system. Another approach is getting passwords and pin codes by using techniques such as phishing. Phishing is a form of criminal activity that uses social engineering methods. It is a fast growing activity that is threatening credit card transactions and other sensitive information that can be easily attacked by cyber thieves. The growing number of reported phishing incidents is shedding light to the importance of protection methods such as user awareness and training, technical measures, as well as laws and legislations stated by the governments or regulatory agencies. Customer awareness' is crucial to fight phishing. McDowell (2012) in ITP.net, stated that "Email phishing defrauds millions of people and companies every year, resulting in a loss of consumer confidence in email and the Internet as a whole," Recently, affiliation between

influential email services, technology providers and financial institutions, such as Gmail, Hotmail, Yahoo, Linkedln, AOL, Bank of America, Paypal and others developed a "standards-based framework" to introduce email authentication technologies into their infrastructure to fight phishing.

According to SPAMfighter News (2006), Bank of Bahrain and Kuwait (BBK) was targeted for phishing. The email included a link which leads the consumer to a fake website where individual's restricted information were explore with which phishers can retrieve the customer account. A look at the phished website tolerates a signal similarity to the original BBK website. BBK management indicated that it is very complicated to monitor the original resource of the attack but the bank conducted customer awareness Campaign "to check scams from claiming victims" and required support of its Internet Service Provider ISP to block the fraudulent websites.

Denial of service: Basically, the term Denial of Service describes the situation when an error occurs and the computer system is not working, or rather not able to provide its intended services. The effects of such a situation can harm a single computer or a whole network, regardless of it being a Local Area Network (LAN), a Wide Area Network (WAN) or a Metropolitan Area Network (MAN). The most mutual methods of Denial of Service (DoS) attacks are carried out through overloading bandwidth utilization, thievery of IT resources such as hardware and software, misusing of defective programming and traffic rerouting.

Recently, TradeArabia (2013) reported from Reuters that Microsoft Corp (Digital Crimes Unit) and the FBI supported by agencies from eighty countries around the world to investigate the worldwide biggest cybercrime rings attack, believed to have stolen more than $500 million by about 1400 malicious computer networks known as the Citadel Botnets from 5 million PCs around the world affecting major financial institutions accounts, including: American Express, Bank of America, Citigroup, Credit Suisse, eBay's PayPal, HSBC, JPMorgan Chase, Royal Bank of Canada and Wells Fargo. Microsoft has filed a court case versus the anonymous hackers in North Carolina while, the USA Federal Bureau of Investigation reported that they are operating directly with Europol and engage international partners bodies to attempt to arrest the unidentified lawbreakers and bring them to the justice. Hence, "The Citadel software is programmed so it will not attack PCs or financial institutions in Ukraine or Russia, likely because the creators operate in those countries and want to avoid provoking law enforcement officials there, Microsoft said".

Hacking: Hacking is defines as unauthorized use or avoidance of security standards or means of an information system or a network. It is as illegal access to other people's computers or systems to damage or abuse its resources. Many laws have been stated to protect people from becoming victims of hackers. Yet, this has not stopped offenders from committing hacking crimes. Financial losses are accounted the most affected losses incurred from hacking activities.

According to Grewal (2011) Iranian and Hizbollah hackers have waged many cyber-attacks to Bahraini governmental websites such as Ministry of Interior (MOI), Ministry of Housing and Bahrain News Agency. The Authorities in Bahrain are claiming that they have all the IT resources to counter any attacks comes from anywhere and have the experience to do so and recorded all IPs that have been used by these hackers. In addition, the government expanded the authorities of the Anti-Economic Crimes Directorate to establish community collaboration to fight "financial and administrative crimes and all forms of corruption". This included Anti-corruption, Anti-cybercrimes, Anti-economic Crimes, Financial Investigation Committee and Interpol Division (GDN, 2011).

Furthermore, Interpol International is getting Bahrain collaboration to develop the Global Complex to fight cybercrimes to improve the government's presence in Asia and scheduled to perform during 2014 in Singapore (GDN, 2013; Interpol, 2013).

COMPUTER FORENSICS

Computer forensics mainly started with the first period a system administrator decided to find out what unauthorized changes had occurred and by whom in his system. Although, the concept is reasonably new, computer forensics can be considered as a branch of forensics. It was first limited to law enforcement divisions and investigators. Sambidge (2012) stated that antigovernment group manages to hack the Gulf Air official Facebook page by replacing the company's logo with positing activist photo. The instance was immediately taken care of by Gulf Air and worked with law enforcement agencies to prosecute those involved.

However, in today's growing advancements, computer forensics tools are available for the public use. Organizations and individuals can conduct cases to investigate any suspected situations of computer crime and thus apply auditing standards and principles.

A clear-cut definition of computer forensics basically includes recovering data from floppy disks, hard drives, or removable disks such as flash memories. Forensic difficulties of compression, encryption, password protection and Steganography have been combined to the overall investigation process. On the hardware side recent additions include up-to-date technological innovations such as smart cards. Handheld devices such as electronic organizers and personal digital assistants can also be considered as possible evidence.

Another place evidential data can be located in and recovered are printers. Some have big stores of memory from which documents have the potential of being retrievable. The printer head, toner cartridge, or ink cartridge may also prove useful as physical evidence to locate specific printouts that were produced from specific printers. A branch of computer hardware which grew out of the requirement to share data faster and the want for centralized servers to store data, is the computer network. As these networks developed and interconnected, the Internet evolved.

There are two general techniques in visualization environments that analysts in forensic cases might use. The first is Non-hierarchal Visualization Techniques: non-hierarchal "views of file statistics display every files in a directory and its subdirectories without any consideration given to the relationship" among "said files and directories". The second is "Hierarchical Visualization Techniques: hierarchical views of file statistics" display "the relationship of files as they exist in the directory structure (Teelink and Erbacher, 2006).

When dealing with computer forensics, the main type of evidence beside the physical type is the digital. Digital evidence is evidence that is kept on or transmitted by computers. It can play a major or a minor role in a wide range of crimes, including homicide, rape, abduction, child abuse, child pornography, stalking, harassment, fraud, theft, drug trafficking, computer intrusions, spying and last but not least terrorism. However, an increasing amount of criminals are using computers and computer networks, few investigators are knowledgeable in the technical and legal matters associated to digital evidence. As an outcome, digital evidence is frequently overlooked, collected incorrectly and analyzed ineffectively.

According to an interview with the Head of Cybercrime Unit in the MOI with TradeArabia (2013), stated, Bahrain Cyber Police draft law which could enforce a maximum penalty of up to US$263,762.00 on hackers. He added that social media misuses are increasing "as hackers seduce young women into sharing private pictures and then post them on pornographic or matrimonial websites" and they argue for the need for more public awareness programs while the governmental

team "of forensic investigators are qualified to deal with new threats and are constantly monitoring any new trends". Hence, he confirmed that, 80% of victims are women. Cybercrime rise 10 fold since the Unit was introduced during 2006 with above 200 cases being registered each year since 2010. During 2010 the Unit registered 223 cases but in 2011 they were 249 cases were reported. Unfortunately, the missuses of social media such Twitter and Facebook has increases the percentages of cybercrimes in Bahrain by creating phony accounts and begin for example, circulating and posting females' information and photos in pornographic websites, use in the wrong way and threating the victims.

Data types: Morris (2003) illustrated three types of data that users might use to hide evidence; nonetheless these data can be used in forensic examinations. The first type is "deleted data", this is basically the data that users delete and believe that it is removed from the system.

This is not true. Even if the user delete files from the recycle bin in the window operating environment, the data is not deleted from the system permanently.

The second type is "hidden data". This is data that the user wishes to store but hide from others. The simplest way to do so is by changing the name or file path by of the file. Another way is by using encryption techniques that will hide the content and sometimes the nature of the designated file.

The third and last type is "system data" which is data stored by the operating system or other software related to operations and transactions occurring within a single computer or even a network. An example of such data is the Cookies folder that is used by internet sites to store information regarding site visits by the user. Examining files containing such data help retrieve and reveal information related to files that existed previously and logging activities to the system. Morris (2003) also describes a specific type of files which are the temporarily files that exist when a process is running or when installation is at progress. These files usually are removed once the application is closed or the system is shut down. Based on his experience, the most significant information related to a user's surfing activities over the Internet is generated by the combination of temporary files developed by the Internet Explorer Web browser and the Cookies file.

Approaches and methodologies: Many researchers and computer forensic investigators argued different steps and approaches taken when conducting a computer crime investigation. Nevertheless, the majority agrees that the bold steps included in such an investigation include: securing the suspected computer, securing the potential evidence, collecting evidence, analyzing evidence and lastly preparing and presenting the evidence. May (2002), suggests some preliminary steps that must be considered before conducting an investigation. These steps include:

- Documenting facts and clues that relate to any useful information for further referencing
- Researching the background and history of computer and suspect
- Establishing a well prepared chronological order of the main players who are involved in the case
- Establishing the level of damage caused by the incident to other computers or networks
- Assess the degree of importance the involved systems are to running the business. If the system is vital to running the business the investigation has to occur outside working hours
- Considering legal positions as well as the option of coordinating with the police
- Allocating a team of expertise to conduct accordingly the investigation and asses the analytical techniques and tools use

May (2002) also noted that "one mistake which businesses often make is that subsequent to an IT crime they make every effort to get systems up and running as quickly as possible, destroying vital evidence in the process". This highlights the importance of the factor of time and how it can affect and question the process of data collection and the integrity of services provided by the business alongside.

Table 1 is adopted from Beebe and Clark (2005) it depicts the importance of setting a clear objective of the investigation: forensic or non-forensic and the main differences of each choice.

After the preliminary actions have been taken once a crime is suspected, the next step in the forensic investigation is conducted: securing the suspect computer. It is important to make sure that evidence allocated on the computer are not tampered with or altered by anyone. Pictures of the alleged crime scene must be taken and descriptive precise notes must be noted as well. Pictures and notes provide a good reflection of the hardware and the connection methods situated. If the computer is a part of the network it has to be removed and the shutdown procedure must be documented.

The next step in the examination process is: securing potential evidence. This is a delicate and a critical issue. The investigator must ensure that the evidence is not contaminated while moving related hardware of the crime or isolating the computer itself. Data stored on the suspected computer must be secured because they are easily targeted by offenders who might destroy the evidence by viruses or such. No one should be allowed to do anything to the suspected computer without the consent of the investigator who should do backups to make sure no data is changed or deleted throughout the investigation process.

The third step involves collecting the evidence. At this stage, deleted files are recovered and encrypted files are decrypted. This is done on copies of the original computer system to avoid updating the changes to the original system and thus losing potential evidences. Next is the step where analyzing of evidences collected is done. The investigator needs to have a keen eye supported with solid evidence to analyze hidden aspects of the collected data.

To finish the investigation the last step is reached: preparing and presenting the evidence. It is important to that the investigator validates and examines the integrity of the collected evidences before submitting them to the court. A solid case must be built on concrete allegations. Documentation plays a major role in this stage. The court will take into consideration all aspects of the investigation to check the reliability and effects forensic evidences hold against the offender.

Forensic tools: The scope and exposure of computer forensics cover a wide range as noted earlier. It includes organizations and individuals. Table 2 lists some examples of computer forensics tools used when conducting investigation (Wang *et al.*, 2005).

Auditing software related to computer forensics range from commercial to free applications. Cost does add efficiency and a more concrete presentation of data and reliability aspects, yet many free tools offer the basic needs to individuals and small cases. The aspect of finding forensic tools free on the Internet, for instance, supporting the idea that the concept of computer forensics is becoming more common than before. The collection of tools available nowadays is continuing to expand and developers are updating them with the latest technologies to support investigations. The investigator must keep in mind the diverse collection of tools available and the most suitable for the case at hand.

Table 1: Example of impacts of differing investigation objectives on server intrusion cases (forensic vs. non-forensic)

	Nature of investigation (forensic)	Nature of investigation (non-forensic)
Evidence preservation principle	Forensic duplicate (s) of compromised system (s)	Copies of log(s) only
	Strict use of write-protection technology	Writes to the evidence avoided; No write-protection technology use
	Positive, legal chain of custody maintained	Positive, legal chain of custody not maintained
	Hashes and checksums maintained on forensic duplicates	Hashes of log files calculated and maintained
	Forensic working copies made and used during analysis by rule	Working copies used as desired for efficiency, not as rule
Documentation principle	Carefully document, interview, statements and impact assessments	Document vulnerabilities from interviews to support system defense
	System state and volatile data carefully/permanently documented	State and volatile data documented for memory and lessons learned
	Chain of custody documented	No documentation of chain of custody
	Process, tools used, findings carefully/permanently documented	Processes, tools, etc. documented for memory/lessons learned
	Information retention policy is long-term focused	Information retention policy is short-term focused
Data collection phase	Logging level increased	Logging level increased
	Forensic duplicate (s) of compromised system (s)	Copies of log (s) only
	Memory dump obtained and forensically preserved	Memory may be analyzed but not forensically preserved
	Additional data capture techniques considered (e.g. wiretaps)	Additional data capture techniques not considered
Data analysis phase	Forensic image sent to forensic consultant for analysis	All analysis conducted in house by trained incident responder
	Focus is on event reconstruction with emphasis on attribution	Focus is on containment, eradication, recovery and lessons learned
	Search for rootkits, rogue processes, "Chron jobs", etc.	Search for missing patches to facilitate better system rebuild
	Events reconstructed by reconciling logs from other systems	Logs from other system only examined to ID other compromises

Table 2: Example of computer forensics tools and software

Name	Platform	Description
EnCase	DOS, windows NT, 2000	Full-featured windows-based computer forensics analysis software that allows a user to image and examine data from hard drives, disk and palm PDAs. Used by law enforcement and private forensic firms (http://www.encase.com)
CRCMD5	DOS	Using MD5 hashing function, primarily for creating a unique hash value for individual file, or all files on a given storage device. It uses 128-bit length key and can easily be run from a floppy disk (http://www.forensics-intl.com/crcmd5.html)
DiskSig	DOS	Same as the CRCMD5, but it is a drive level hashing program for verifying the accuracy of evidence grade backups of hard disk media (http://www.forensics-intl.com/disksig.html))
Safe back	DOS	Primarily for imaging a hard drive and restoring the image to other hard drive. It can be run from a floppy disk. Used by law enforcement and private firms (http://www.forensic-intl.com/safeback.html)
@Stake LC4	Windows NT/2000	Passward auditing and recovery software (http://www.atstake.com/research/lc/)
WinHex	Windows NT/2000/XP	Disk editor for hard disks, CD, DVD, ZIP, smart media and compact flash memory cards. FAT12, FAT16, FAT32, NTFS, CDFS (http://www.sf.soft.de/winhex/)
Word list	Windows NT/2000	A good source for dictionary attack password cracking (http://www.outpost9.com/files/wordLists.html)
Windows secret explorer	Windows NT/2000/XP	It allows exploring and editing windows protected storage, locating hidden information in any windows-based system. Retrieving data enter to web page, web passwords, dial-up passwords and other data stored by Microsoft in the protected storage (http://lastbit.com/wse/default.asp)
Photo rescue	Windows 95/2000/NT/XP	Basic digital camera photo recovery software can be used with crashed or accidentally deleted files (http://www.wildlifephoto.net/howto/photorescue.html)
Solitaire forensics kit	DOS and Windows 95/2000/NT/XP	Portable hard drive duplication kit used by FBI for duplicating and imaging hard drives (http://www.logicube.com/)

The economic impact of cybercrimes in business: According to Savona (2012) in the Global Council on Organized Crime report stated that, organized crimes suffer the loss of a multibillion cost on legal business, damages markets and affects extensive outcome on community. Accelerated through the equivalent strength of worldwide that involve extended business, global information and communications, criminal groups nowadays have extraordinary reach into the lives of normal citizens and into the boundary of international corporations and public organizations globally.

The estimation cost of cybercrimes are very difficult to authenticate, nevertheless a study by Norton Cybercrime (2011) reported that cybercrime cost 24 countries (UAE was the only Arab country among these selected countries for survey) Internet users US$388 billion worldwide. The amount encompasses US$274 billion in the time lost and US$114 billion for recovery. About 30% of surveys participants consider to a greater extend to be a target of cybercrime than physical globe crime.

Nevertheless it is estimated the cost of the global cyber activity to be between $300 billion to $1 trillion and in the USA alone between $24 billion to $120 billion.

It necessitate us all to work harder toward raising awareness, to enhanced security, to be further alert and to dedicate more in our cyber smarts and protection.

According to Gartner's latest report, news 24/7 sheds light on how the financial impact of cybercrime will increase 10 percent per year because of the continuing discovery of new vulnerabilities.

The report also articulated that new software vulnerabilities might arise and innovative attack paths would be developed by financially motivated attackers, as IT delivery method continues to meet the demand for the use of cloud services and devices owned by the employees. The combination of new vulnerabilities and more targeted attacks will lead to continued growth in bottom-line financial impact because of successful cyber-attacks. Gartner, Inc. has also revealed its top predictions for IT organizations and users for 2012 and beyond.

A warning came out from a leading financial security expert who believed that small Bahraini banks could face attack from international criminals.

Tony tesar, a Bahrain based financial security specialist Chief executive, stated that these recent events are continued proof that the crimes in banking sector are moving away from physical attacks to a harmless more financially profitable tactics of doing it remotely. Further to which he also mentioned that the ability to secure data on participant has never been more relevant and the use of effective firewalls has never been more critical. The need to on a regular basis tryout online orderliness and servers will be requirement in conflict these cases of pick apart and smaller banks with less effective make up one's mind will always be more prone to attack. These types of attacks are very unmanageable to foreclose and discover due to continuous advances in technology and the speed at which an attack can take social rank. Regular penetration testing (Pentesting) is essential and using a variety of organizations and individuals to assist with this will greatly help in staying ahead of advances in technology and in identifying loopholes and gaps in a bank's existing online and internal IT systems.

Mr Tesar said an alternate thought is the monetary and reputational effect it will have on the banks that are casualties of this sort of strike. Having adequate security methods set up and complete emergency administration and fiasco recuperation plans, will extraordinarily support in managing these sorts of assaults and the fallout that will accompany.

Meanwhile, Union of Arab Banks chairman Adnan Yousif said Bahrain-based banks are well protected from any cyber-crimes, reports our sister paper Akhbar Al Khaleej. They are sheltered

from such ambushes in light of the fact that they utilize European advances starting from major worldwide organizations, including the sound supervisory approaches actualized by the Central Bank of Bahrain have helped raise a protected keeping nature's domain.

Impact of cyber-crimes in business on a global scale: The 2011 Norton Cybercrime showed that over 74 million people in the United States were preys of cyber rimes in 2010. The direct financial losses caused by these types of criminal acts were $32 billion. About 69 percent of adults online have been victims of cybercrime resulting in 1 million cybercrime victims a day. Many people have the attitude that cybercrime is a fact of doing business online.

"Gary Warner, director of computer forensics research at the University of Alabama at Birmingham, has been quoted as saying that the fight against financial cyber-crimes is that the criminal complaint has almost disappeared. Even when a police report is filed it is often "so the bank will give you your money back."

The cyber Intelligence identified that a decently huge and composed that is said to be utilized false wire exchanges as the method of strike. This digital security strike is said to influence session capturing in a man-in-the-middle cyber assault. Subsequently, Man-in-the-middle cyber-attack is characterized as a bargain where the assailant has the capacity to embed themselves between its target and the framework or administration in which the target is attempting to enter or utilization. An attacker finishes this by mimicking the framework or administration that the target is endeavoring to interface with by erroneously rerouting the movement to and from the administration or by commandeering session information. Different cyber intelligence sources have cautioned that an expected 30, U.S. based financial services institutions may be the focuses of an arranged cyber-criminal gangs that is said to be the element behind this strike.

As of late, the FBI issued a cautioning about dangers occurring as to cyber-crimes. Their cautioning expressed that the hoodlums behind this cyber-strike were utilizing numerous strategies to acquire client log-in accreditations. When the offenders have these qualifications, they start universal wire exchanges.

Reports being distributed in 2012 showed that cybercrimes have had a twofold digit development and are around the four greatest wrongdoing risks everywhere throughout the world, inside stake robbery unlawful acts, misrepresentation and debasement. These patterns are the same everywhere throughout the world. Cybercrime industry has been gathering a ton of triumph throughout the previous five years. This sector of crime doesn't realize the word "crisis". Actually the cybercrime's financial and geographic development demonstrates no slowdown despite the global economic difficulty.

The lack of awareness have played an important role in the favor of cybercrimes therefore, no organization or company is immune to such crime. Another reason that was found was the inadequate protection measures against crimes as such, taken by organizations which are the leading cause of cybercrime.

Figure 2 illustrate a recent norton cybercrime report costing fraud "victims more than $388 billion worldwide over the past year, consider that up 35% of the global cybercrime bill were U.S. fraud victims, who spent $139 billion on cybercrime last year. An amount of 141 victims per minute is an alarming statistic even for Norton's consumer cybercrime expert, Helen Malani."

Figure 3 shows the Cybercrime and its impact on private Industry while Fig. 4 illustrate average annualize cost by industry sector.

Fig. 2: Norton cybercrime 2011 report

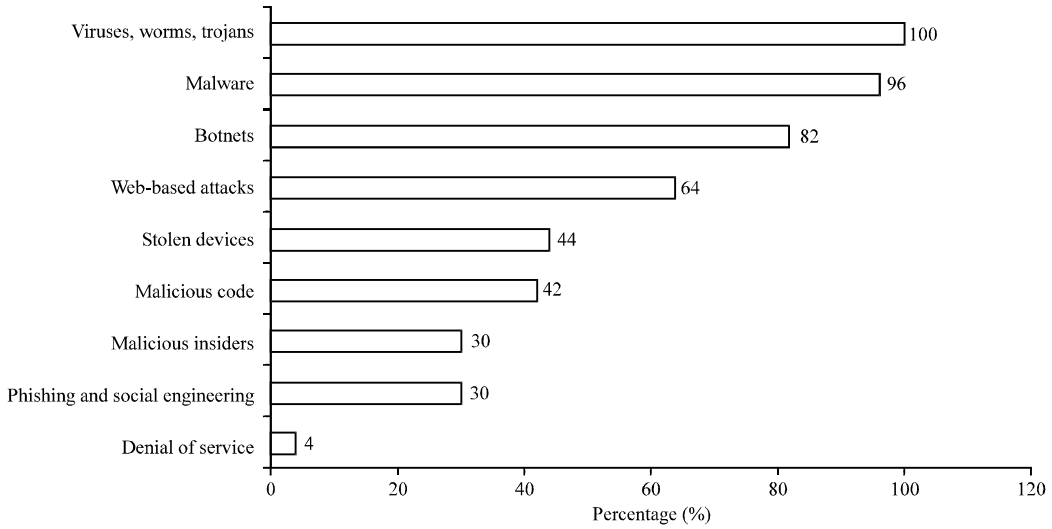

Fig. 3: Frequency of cyber-attacks experienced by benchmark sample

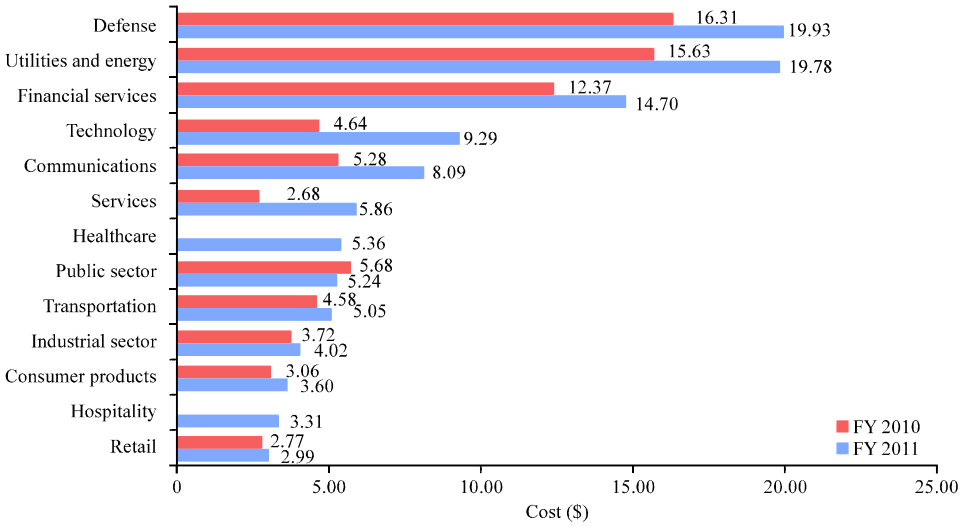

Fig. 4: Average annualized cost by industry sector

There are three sorts of cybercrimes utilized by the criminals; they are Intrusive, silentand dangerous. Regularly the organizations/companies don't understand that they have been casualties of fraud or assaults until long after the crime has taken place. This sort of crime is called silent crime which turns into a major issue while battling such dangers. The outcomes are incapacitating and recover the circumstances is now and then unimaginable, precisely due to the time crevice between the criminal event and it revelation gives favorable element to the individuals who carry out law violations are often unbridgeable that makes it inconceivable for any actions of persecution. Numerous organizations are indeed throughout the years casualties of cybercrime yet are not familiar with it its a tumor that wrecks from inside.

According to the report "Second Annual Cost of Cyber Crime Study-Benchmark Study of U.S. Companies" published by the Ponemon Institute, a study is based on a representative sample of 50 larger-sized organizations in various industry sectors, despite the high level of awareness of the cyber threat the impact of cybercrime has serious financial consequences for businesses and government institutions. The report shows that the median annualized cost of cybercrime for 50 organizations is $5.9 million per year with a range of $1.5 million to $36.5 million each year per company. The total cost is increased if compared to the first study of the previous year.

Greater part of cyber-attacks are generally alluded to a criminal activity led through the web that incorporate cyber espionage that is seizing bank accounts, making and disseminating viruses to infect the exploited people, posting confidential business information on the internet and disrupting a country's critical national infrastructure.

The chart above exhibits that virtually all companies encountered attacks moved using malware. The information likewise shows the actions made by the insiders and the damages initiated by social engineering attacks. Taking everything into account, industries that fall victims to cybercrime have diverse degrees of criminal acts and distinctive economic impact. Defense, utilities and energy and financial service companies experience higher cost than organizations in retail, hospitality and consumer products.

The information being given shows an agreeable circumstance in regards to the effect of the cybercrime on the business of large companies. Nonetheless, huge effect is observed on the small business where the organizations confront the cyber threat with fewer assets and tolerating the dangers related to exposure.

In this market segment cybercrime is exceptionally furious and every day it tries to evade defenseless organizations that regularly neglect to meet the cyber threat, the related damages are destroying causing in many situations the end of the business. In this sector is desirable for governments to support small businesses in harmony with a cyber-strategy defined at the national level. Leave powerless the social fabric made up of small organizations has doubtlessly an immediate affect also on the business of large firms.

Cyber-crime globally: Figure 5 shows a study that has been conducted in the US for three years including other countries as UK, Germany, Australia and Japan. The figure shows an estimated average cost of cybercrimes for five country samples after conversion into US dollars. There is significant variation among companies in the benchmark samples. The US sample reports the highest total average cost at $8.9 million and the UK sample reports the lowest total average cost at $3.3 million. Possible reasons for these differences could be the types and frequencies of attacks experienced as well as the importance that each company places on the theft of information assets versus other consequences of the incident.

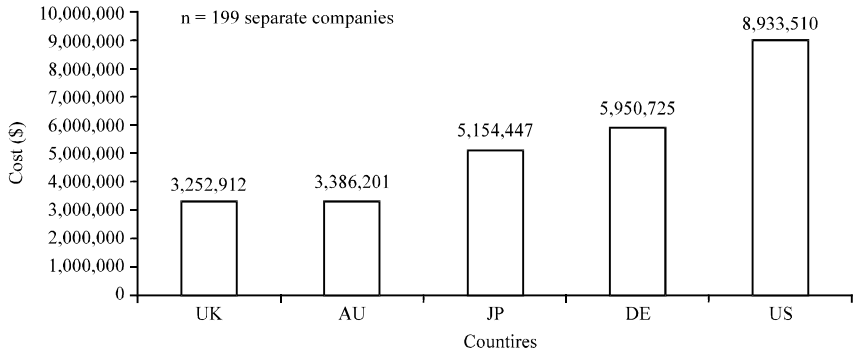

Fig. 5: Cost of cyber-crime globally

It was found that US companies were much more likely to experience the most expensive types of cyber-attacks which are malicious insiders, malicious code and web-based incidents. Similarly, UK and Australian were most likely to experience denial of service attacks. In contrast, German companies were least likely to experience malicious code and denial of services. Japanese companies were least likely to experience malicious insider and web-based attacks.

Another key finding that may explain cost differences among countries concerns the theft of information assets. US and German companies report this as the most significant consequence of a cyber-attack. On the contrary, UK and Australia cite business disruption as more important. Business disruption can be less costly than theft.

BAHRAIN STATUS IN CYBERCRIME DATA ANALYSIS:NUMBER OF REPORTED CYBER CRIMES CASES IN BAHRAIN

This section is based on an actual data collected from the MOI, Department of Cybercrime reported cybercrimes.

According to the MOI number of reported data illustraed in Fig. 6 shows an accurate number of unpublished cases reported under cyber crime as a whole from the year 2008-2012. As illustrated in the Fig. 1, the number of cases reported is increasing rapidly as years pass. In 2008, 73 cases were reported and by the next year 2009 an increase can be seen on the number of reported cases. Cyber crime reports was at a peak in 2011 with a total of 239 cases which reduced later to a total of 232 cases in the year 2012.

Number of reported e-mail theft and breaking through cases: Figure 7 illustrates number of reported e-mail theft and breaking thruough cases.

Email Theft and Break Through cases are considered the most common type of cyber crimes. These are commonly financial in nature. Cyber criminals hack into personal financial accounts to access funds. They attack website databases in order to gain access to consumer details, such as Social Security numbers, that can be used to take out credit cards or loans in another person's name. This can be done either through hacking or creating a web page that is very similar to the orignal website in order to get information such as E-mail ID's and Passwords.

Figure 6 above illustrates that in 2008 the number of reported cases regarding email theft and breaking through were only 6. The possible reason for such a small number could be that these 6 reported cases must have been a very serious one. On the other hand, people do not report such cases as long as they have nothing important in their accounts to lose and go on to create new email

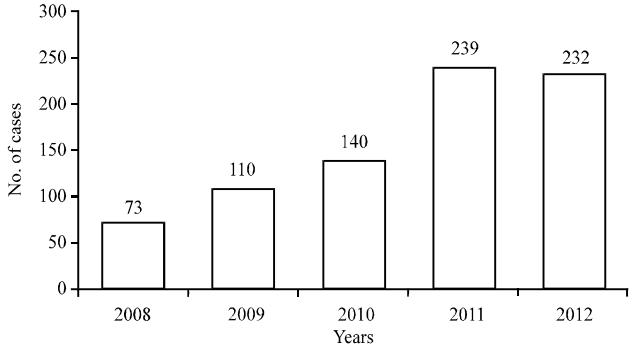

Fig. 6: No. of reported cybercrimes in Bahrain from 2008-2012

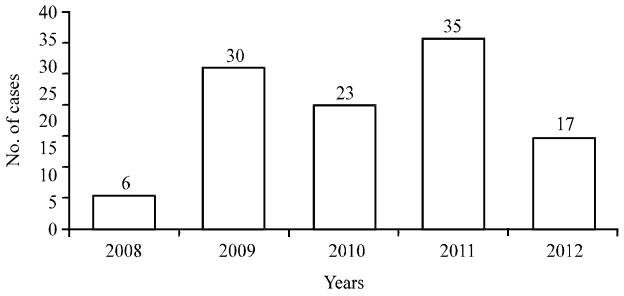

Fig. 7: No. of reported e-mail theft and breaking through cases

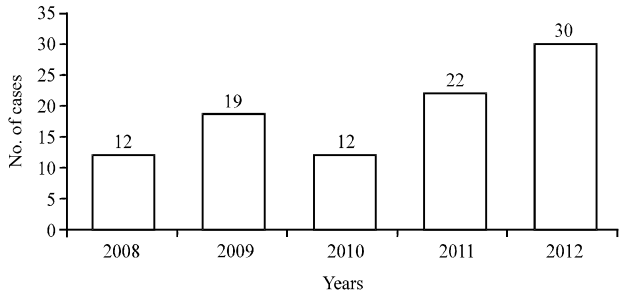

Fig. 8: No. of reported threat cases

id's. In 2009, the number of reported cases rapidly increased to 30 and by the year 2010 it dropped to 23. In 2011, the number of reported cases was at its highest with 35 cases being reported. It is evident from the figure that the number of reported cases fluctuate from one year to another.

Number of reported threat cases: Figure 8 shows the of reported threat cases in Bahrian and reported to the MOI.

Threat cases usually involves threat to a person personal information, bullying, harrasment and, stalking. There are several high-profile cases of threat, where a person is bullying or harrasing someone over the internet. For example, a bully can post unwanted pictures or harsh messages about the victim on social media websites like Facebook, or upload embarrassing videos of them on Youtube just to play with their emotions. Harassers and bullies may also steal their victims' passwords, to impersonate them on the Internet or monitor their e-mail accounts.

Figure 8 above shows that in the year 2008 the number of reported cases according to the MOI was 12 and it increased in the year 2009 by 19 cases being reported. In 2010 the reported cases was similar to the year 2008. By 2011 the number of cases involving cyber threat was increasing at a higher pace with 22 cases being reported. The year 2012, where about 30 cases were reported, marked the highest number of threat cases.

Number of reported abuse cases: Figure 9 shows the number of reported abuse cases to the MOI.

Cyber abuse is the use of the Internet to harm or harass other people in a deliberate, repeated and hostile manner. Unlike physical abuse it can remain virtually anonymous using temporary email accounts, false name in chat rooms, instant messaging programs, cell-phone text messaging and other Internet venues to mask their identity; this perhaps frees them from normative and social constraints on their behavior.

In 2008 there were no such cases reported which later on increased to 5 cases in the year 2009. As we can see from the chart these cases started to increases drastically with 13 cases in the year 2010. The number of cases reported were 24 and 23 cases in the year 2011 and 2012, respectively.

Number of reported dum cases: Figure 10 illustrate number of reported cases of dum to the MOI. Dum cases were common in the earlier years as we can see that there were 19 cases reported in the year 2008. Which later on increased to 25 cases in 2009, 38 cases in 2010. 2011 and 2012 shows us that the number of reported Dum Cases increased majorly with 78 and 85 cases, respectively.

Number of reported disturb cases: Figure 11 illustrate the number of repored disturb cases. Disturb cases have been one of the cases were only a few were reported yearly. In the above chart

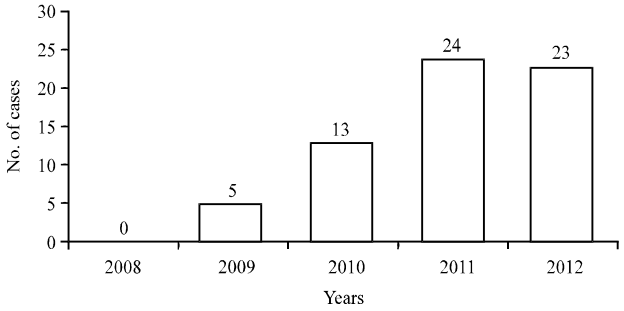

Fig. 9: No. of reported abuse cases

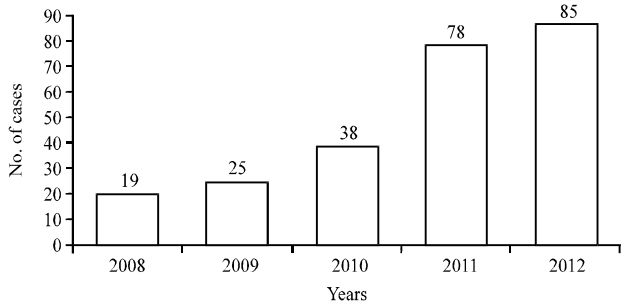

Fig. 10: No. of reported dum cases

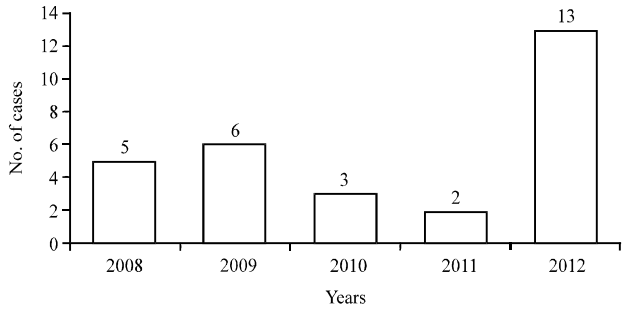

Fig. 11: No. of reported disturb cases

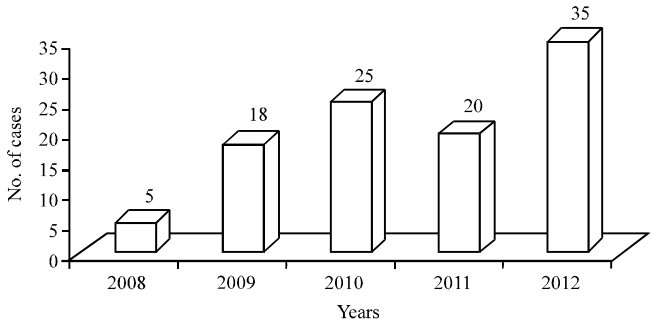

Fig. 12: No. of reported libel-insults cases

we can see that 5 cases were reported in 2008, 6 in 2009, 3 in 2010. In 2011 this has decreased a little to just 2 cases in a whole year. Whereas in the year 2012 it has increased to a total of 13 cases being reported.

Number of reported libel- insults cases: Figure 12 shows that number of reported label libel-insuite cases to the MOI. Cyber or online defamation is considered to be as, if not more harmful than defamation in the form of libel and slander in the brick and mortar, physical world. In some cases, the effects of online defamation could be exponentially worse than an offline incident due to the global nature of the Internet and the fact that the statements can be accessed by virtually anyone. In addition to this, the issue of anonymity online raises even more concern when dealing with defamation because the author or origin of the statements may be very difficult to trace depending on the medium.

In short, the Criminal sends emails containing defamatory matters to all concerned of the victim or post the defamatory matters on a website. (Disgruntled employee may do this against boss, ex-boyfriend against girl, divorced husband against wife etc.).

Cyber defamation has been increasing from the year 2008 onwards with a number of reported cases being 5 which later on increased to 18 in 2009. In the year 2010 there were a total of 25 cases reported under this type of cybercrimes. In the year 2011 it was reported that the number of cases reported under cyber defamation reduced to 20 cases. In 2012 the number of cases increased majorly with a total of 35 cases being reported.

RECOMMENDATIONS AND LIMITATIONS

Recommendations include conducting interviews regarding the topic of computer forensics with people whom have been victims or have investigated in relative cases. Another recommendation

is conducting a quantitative study to measure the degree of awareness of the society in the Kingdom of Bahrain concerning cybercrimes and investigations involved with computer forensics. Limitations in this study were due to the lack of computer forensic cases that occurred in the Kingdom of Bahrain. Even if some cases did occur, they were classified as confidential cases and public access to related case documentations was prohibited.

CONCLUSION

Daily advancement in Information Technology are benefiting with no doubt human lives. However, these progresses come at the cost of computer crime and abuse. This downside of technology affects the overall usage of it and the way technologies are perceived by users. Computer forensics is a moderately new concept that has emerged to help identify the offenders and computer crime committers. This offers an assuring sense of security for individuals and organizations, thus allowing them to provide the best outcomes and productions along with services to the society.

REFERENCES

Al-Alawi, A.I. and M.F. Abdelgadir, 2006. An empirical study of attitudes and opinions of computer crimes: A comparative study between U.K. and the Kingdom of Bahrain. J. Comput. Sci., 2: 229-235.

Beebe, N.L. and J.G. Clark, 2005. A hierarchical, objectives-based framework for the digital investigation process. Digital Invest., 2: 147-167.

CSI, 2011. 15th annual computer crime and security survey. Computer Security Institute.

GDN, 2011. Cabinet push to fight cybercrimes. Gulf Daily News, Bahrain, September 19, 2011. http://gulf-daily-news.com/NewsDetails.aspx?storyid=313726.

GDN, 2013. Help sought for cybercrime cell. Gulf Daily News, Bahrain, February 19, 2013. http://www.gulf-daily-news.com/source/XXXV/336/pdf/page09.pdf.

Grewal, S.S., 2011. Fighting cyber crime. Gulf Daily News, Bahrain, May 03, 2011. http://www.gulf-daily-news.com/NewsDetails.aspx?storyid=305199.

Interpol, 2013. Enhancing international law enforcement cooperation and training focus of INTERPOL Chief's visit to Bahrain. February 18, 2013. http://www.interpol.int/News-and-media/News/2013/PR015

May, C., 2002. Computer forensic: The morse or clouseau approach. Comput. Fraud Security, 2002: 14-17.

McDowell, B., 2012. Tech companies collaborate to fight phishing. http://www.itp.net/popup/print/587806

Morris, R., 2003. Uncovering a user's hidden tracks. Comput. Fraud Security, 2003: 11-13.

Norton Cybercrime, 2011. The shocking scale of cybercrime: Report. http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/

SPAMfighter News, 2006. Phishers target bank of Bahrain and Kuwait. SPAMfighter, Denmark. http://www.spamfighter.com/News-6307-Phishers-target-Bank-of-Bahrain-and-Kuwait.htm.

Sambidge, A., 2012. Bahrain's gulf air says facebook page hacked. April 10, 2012. http://www.itp.net/588577-bahrains-gulf-air-says-facebook-page-hacked#.Ufm1053frIV.

Savona, E.U., 2012. Organized crime enablers, Global council on organized crime. World Economic Forum, July 2012. http://reports.weforum.org/organized-crime-enablers-2012/#chapter-enablers- of-cybercrime

Teelink, S. and R. Erbacher, 2006. Improving the computer forensic analysis process through visualization. Communi. ACM., 49: 71-75.

TradeArabia, 2013. Cracks down on cyber crime. TradeArabia Business News Information, Bahrain, January 12, 2013. http://www.tradearabia.com/news/IT_228801.html.

Wang, Y., J. Cannady and J. Rosenbulth, 2005. Foundations of computer forensics: A technology for the fight against computer crime. Comput. Law Security Report, 21: 119-127.