Study of the Cybercrime Cost and the Risk of Criminal Threats to the Banking Sector

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

Ms. Sara Abdulrahman Al-Bassam
Arabian Gulf University, College of Graduate Studies,
Department of Innovation &amp; Technology Management
Arabian Gulf University,
P.O. Box 26671, Kingdom of Bahrain

Abstract:

Purpose: This study focuses on cybercrime cost, losses and the risk of criminal threats to the banking sector and how to minimize the risk of crime threats to the businesses. Literature indicates substantial financial losses suffered by numerous corporations in different countries due to the criminal breaches committed in cyberspace. The crisis of cybercrimes has been cultivated into a global environment; to elaborate a scientific method of resolving this dilemma, it is crucial to formalize the separation and classification of the key objectives of the critical properties of the matter. Nevertheless, continuous employee awareness program is the major contributing factor in the bank security culture. Via education and awareness, all staff can be equipped to act as a human firewall to defend any attack.

Design/methodology/approach The study examined the data concerning the costs and losses caused by cybercrime that are available in literature and studies from the Gulf Corporation Council countries and worldwide examining the valid causes of such harms. Additionally, Quantitative research method use and out of 168 self-administrated questionnaires 119 IT employees responded and ten questionnaires were rejected because they were not completed

Findings: When the participants were asked how knowledgeable they are about security risks, about 46% indicated that they are between somewhat knowledgeable to not knowledgeable. This indicates the need for the execution of security risk knowledge, awareness and training. The board should play a significant role in driving the IT strategy, given its importance in corporate strategy. This should cover every dimension of the management of technology systems. That is to say: cost, human capital, hardware and software, vendors and service providers, and risk management, including disaster recovery, should be factored in the IT strategy of the bank. Malware comes in the first ranking of threats that have the most increased banks' risk exposure over the last 12 months, the second comes spam and the third-ranking comes phishing. Almost half of the respondents indicated that they do not have a nay specialized professional IT security certificates, this is a clear sign of lack of interest in training courses that raise the level of awareness and progress in the field of rapid technical change.

Practical Implications: While the budget is the financial facility, which firstly rationally estimates the costs and secondly assesses access to the resources required to achieve successful implementation of cybersecurity. By remaining familiar with the causes that banks may determine it clear-cut to indicate to invest in security against attacks from cyberspace and enhance their proficiency with minimum costs.

Originality/Value: This study reports the cost and risk of criminal threats to the banking sector and how to minimize them. As breaches and breaking the law electronically are becoming more complex; they cause a further financial effect on the banking sector. The management should have a better understanding of the rise issues. Therefore, once a business faces some challenges and has been exposed to a particular risk, the bank has to act fast and prepare its security plans. Such plans may be a considerable investment, so it is crucial for the business to balance its security costs and to be full.

Keywords: Cost, Risk, Cybersecurity Awareness, cyberspace, cybercrime, criminal

Introduction

In connection with different types of threats, there are various types of attacks used. These can affect business information today mainly through worms, viruses, denial of services, access and reconnaissance. Cybercrimes encountered can often include crackers, spammers, phishing and hacker attacks (Zadig, 2016; Al-Alawi et al. 2020a).). In fact, some certain people or organizations may gain benefits from threatening the firm's assets information. These could include the company's former employees or people with whom the firm does business. The negligence of an employee who has accidentally compromised the firm's data, or other business competitors who want to penetrate other profitable firms to gain economic advantage, all comprise cybercrime risk for the organization. This may involve disruption of the business of trading, especially for those who conduct their business online, causing them financial losses due to the theft of information, which, therefore, will result in the firm paying costs for data breaches. For other related costs for such incidents, such as a firm losing its reputation, and its customer base, and incurring costs for cleaning as well as running their affected system, costs for the damages suffered by other companies that are connected to the affected firm, and additional costs of fines for any other personal data losses.

The Main Objective of Cybercrime

Consequently, cybercrime's main objective is to affect the IT equipment or IT-based services of government or businesses for the reason of either obtaining money or affecting reputations. This is done by penetrating the company's IT equipment to affect their valuable asset information, which mainly contains the data related to the databases of customers and their financial details. Hence, their client list, the firms' pricing information and the dealings they have with other companies. The firms' product design, as well as their manufacturing process, are all valuable information mainly stored in the firm's IT systems, which may be affected by cybercriminals (HM Government, 2015; Arlitsch & Edelman, 2014, Al-Alawi et al. 2020b).

In addition, one of the causes for cybercrimes in society refers to the concept of whenever the rate of investment return is high and its risk is low. Many people will have the advantage of such a situation and this means that accessing and trying to use the valuable information acts as a high yield of return. Hence, stopping and catching those criminals is difficult, which explains the increase of cybercrimes in many societies (Al-Alawi, 2014, Al-Alawi, et al. 2020).

SEL (2015) has stated some advantages of using cybersecurity in organizations:
First: providing a layer of protection and security for efficient access to the firms' data. Second: improving the software and operational efficiency tools to authorized users. Third: keeping the firms' network system directly connected to the adopted security rather than depending and relying on other securitized ways that may lead to catastrophic data theft or loss.

According to HM Government (2015), there are some actions or procedures that organizations should adopt to ensure the safety of their sensitive information and data. Moreover, to minimize the risk of crime threats to the businesses, downloading software security updates as soon as they are performed and available will keep the company devices safe. The firm should make up strong passwords, to avoid unauthorized access, from encryption, deleting emails that seem suspicious as they may contain viruses (as viruses or malware may lead to devise infection, anti-virus software must be used). Last but not least, each business should train its staff and make them aware of cyber threats and how to prevent such threats (Al-Alawi et al. 2020a).

In this regard, as new information technologies, communications are developed to meet and facilitate consumer demand. They play a vital role in the developing countries, where many sectors try to benefit from such applications, especially concerning government, health sector, education, and business, whereby these sectors need to protect themselves from data breaches or destruction by criminal attacks. First, the country's government should provide its citizens with free access to their data, and restrictions will only be imposed in certain situations or significant events. Second, the country is committed to protecting its citizens in cyberspace and the country should apply a code of conduct for information in cyberspace, with the government supporting the effort of the International Telecommunication Union in ensuring the law in the area of cybercrime. Third, the countries' governments and organizations should maintain and have the best use of a cybersecurity program to provide security as well as the privacy of their information. Fourth, people who are experts in producing hardware and software should attempt to develop and improve secured technologies. Fifth, the country's government should actively work on participating in security awareness programs to ensure cyber stability (Armencheva & Smolenov, 2015; Al-Alawi & Al-Bassam, 2019).

Cybercrime Cost

Cybersecurity and cybercrime are two topics that cannot be separated in an interconnected environment, and they will continue to grow. Unfortunately, cyberattacks continue to grow over time and are increasing risks to organizations. Once a business faces some challenges and has been exposed to a certain risk, the company has to act fast and prepare its security plans. Such plans may be a considerable investment, so it is crucial for the business to balance its security costs and to be fully aware of the real costs of cyberattacks. Ghorsad (2014) stated, “The fact that the 2010 UN General Assembly resolution on cybersecurity35 addresses cybercrime as one major challenge underlines this.” The crisis of cybercrimes has been cultivated into a global environment; to elaborate a scientific method of resolving this dilemma, it is crucial to formalize the separation and classification of the key objectives of the critical properties of the matter.

As breaches and breaking the law electronically are becoming more sophisticated, they cause a further financial effect. The Ponemon Institute (2014) survey illustrated that the average cost of cybercrime for American retail shops increased twofold from 2013 to a yearly average of US $8.6 million per corporation in 2014, harming more than was expected. Furthermore, the study indicates that the security incidents will continue to grow to 42.8 million worldwide, whereas PWC (2015) stated that identified information security circumstances have increased from 2009 by 66% every year.

Marden (2017) stated that globally, Juniper Research indicated the costs are expected to increase between 2019 and 2015, with an estimate of $2.1 trillion. The effect would be significant for smaller businesses, as a study by NCSA indicated that 60% of these types of companies reported bankruptcy within six months of an attack. Another projection by Kaspersky Lab is that the average direct costs of a security breach are $38,000 on smaller businesses.

Another global study in seven countries accomplished by the Ponemon Institute (2015) and sponsored by Hewlett Packard Enterprise. The study indicated that the total average costs of cybercrime were, for the USA alone, $18.42m, indicating the highest among these countries, and Russia $2.37m showing the lowest and the others five countries from highest to lowest, Germany $7.5m Japan $6.81m, UK $6.32m, Australia $3.47m, Brazil $3.85m. The seven countries studied summarized that the total number of attacks used to measure the total cost was 1,928, and the average yearly costs were $7.7 million. Hence, there is a significant variation in total cybercrime costs among the enterprises studied around the world. The financial services sector (retail banks, insurance companies, brokerage, and credit card firms) was the most significant sector represented, with 16% out of the total of 252 organizations.

Furthermore, Morgan (2016) reported that cybercrime is driving the IT market for more cybersecurity products and services, which is estimated to grow from “$75 billion in 2015 to $175 billion by 2020”. New markets such as cyber insurance are inspired and enhanced due to cybercrime issues, and predicted to increase from “$2.5 billion in 2015 to $7.5 billion by 2020”.

The Ponemon Institute in its annual study in 2017, sponsored by IBM and including 419 companies in 11 counties and two regional samples (Saudi Arabian and United Arab Emirates ‘UAE’ for Middle East and four Asian countries). The study reported that the global average cost of data breach decreased by 10% over the last year to $3.62 million. In addition, the average cost of each piece of missing data holding confidential information also notably dropped by $17 ($158 during 2016 and $141 in 2017). Nevertheless, despite the decrease in the overall cost, enterprises in this year’s report have higher breaches; the mean size of the data breaches has grown by 1.8% to over 24,000 records. The average total organizational cost in the USA was $7.35 million, and $4.94

million in the Middle East (Saudi Arabia and UAE). The most significant major increase in the average total cost happened in the Middle East (+.83), the United States (+.66) and Japan (+.52). Moreover, the cost engaged for "post-data breach response activities" was $1.56 million for the USA and $1.43 million for the Middle East. These countries (USA, Saudi Arabia, and UAE) were reported to spend more on this cost, which covers such aspects as the inbound communications, legal expenditures, and specialized investigative activities.

Furthermore, the highest direct per capita cost was equal for both Canada and the Middle East (both $81) and these costs were, for example, for hiring a law agent/forensic professional. At the same time, the USA had the highest indirect per capita cost of $146. In addition, the USA had 52% of breaches, and the Middle East (Saudi Arabia and UAE) 59% of the breaches due to insiders, hackers and criminals (Ponemon, 2017). In addition, it is reported that 2/3 of MENA businesses lack cybersecurity policies despite the fact they are claiming that technology is appropriately applied in their workplaces. Moreover, in 2017, the MENA region was affected by the WannaCry virus as well, and most Middle East organization's computers were shut down. According to Kaspersky lab analysis, UAE, Egypt, KSA, Iran, Jordan, and Qatar computers were infected by this virus, but the attacked organizations are still unknown, considering that most MENA organizations are not forced by the law to report about any cyber-attacks.

Furthermore, the size of the cybersecurity market in MENA is predicted to increase from 5.2 billion dollars to 9.5 billion dollars. However, the general costs of cyber-attacks can be losing the intellectual properties, losing the sensitive financial data, spending more money to secure the organizations' networks, the significant cyber-attacks recovery costs, and losing the organizations' reputations. Table-01 illustrates the summary of the cost of top cybercrimes in GCC.

Table-01 Cost *of top cybercrimes in GCC*

Year	Victim	Incident details	Cost
August 2012	Saudi Aramco National oil company of the Kingdom of Saudi Arabia	The assault spread to 30,000 Aramco workstations, and Shamoon malware affected the whole system to close itself from the external world and the system was wiped before crucial harm could be executed. This circumstance caused over 55,000 Saudi Aramco workers to stay home (Perlroth, 2012; Bronk & Tikk-Ringas, 2013; Axelrod & Ilive, 2014; Pagliery, 2015; Bertram & Waters, 2016).	Not declared
August 2012	Qatari natural gas company (Ras Gas)	Was hit with a similar Shamoon virus that shut down its website and e-mail servers. Was hit with a similar Saudi Shamoon malware that blacked out its website and e-mail servers. This attack is to be one of the biggest damage to oil makers. (Maggio & Cacciola, 2012; Security Middle East, 2015).	Not declared
December 2012	UAE ATM National Bank of Ras Al Khaimah	Where the hackers broke into installment preparing organizations utilized by the bank and raised the equalizations and withdrawal confines on the cards, personal account details of users as prosecutors said (Reuters, 2013; Tahoun & Maklad, 2015).	$6 million
February 2013	Oman ATM Bank Muscat	Turkish hacker Ercan Findikoglu who was blamed for stealing US$40 million in a heist utilizing cards issued by Oman's Bank Muscat in 2013, has conceded in a government court in New York. He confessed to five tallies, including PC interruption connivance, for driving a plan that prompted stolen charge card information being conveyed around the world. The US$40 million was stolen in less than 24 hours from Oman’s Bank of Muscat (Nagraj, 2016; Fielding-Smith, 2013).	$ 40 million

Year	Victim	Incident details	Cost
30-Jun 2015	UAE Banking Websites	The well-known coordinated series of cyber-attacks known as hacktivist group anonymous managed to cripple the operations of several major UAE banks. Customers could not access their banks because their targeted banks could not process payments. Customers were not able to perform any financial transactions or checks. During the peak, the busy period was the maximum disruption. Lack of access and security resulted in the loss of reputation (Singer & Friedman, 2014).	Actual funds not stolen in this incident. Undermined cost of the targeted banks. In terms of lost revenue potential losses, customer relation damage remains significant.
September 2015	Aramco /Oil and Natural Gas Corp. (ONGC).	Saudi Aramco foiled US$30.3 million scam due to the Indian cybercriminals who replicated the official email address of the national firm known as Oil and Natural Gas Corporation (ONGC) with small changes and used it to encourage Saudi Aramco to transfer the money to their account. The original email was patel_dv@ongc.co.in, while the fake one was patel_dv@ognc.co.in, and by not noticing the difference, the fraudsters then sent an email asking for the amount to be credited to the Bangkok-based account (Arab News, 2015).	$30 million
Nov 2015	A Sharjah-based Invest bank	The hacker called (Buba) attacked a large bank in the UAE and threatened the bank with the release of the customers' data after they refused to pay a Bitcoin Ransomware worth US$ 3m. The unknown hacker dumped tens of thousands of records on the web, and he started to release sensitive data via Twitter accounts such as credit card numbers and authorization codes for transactions (Metzger, 2015; Thomas, 2015).	500 customer's data has been released to the public, which caused a lot of losses to the customers and the bank's reputation.

17 Nov 2016	GACA Shamoon Attack	Shamoon malware attack wiped out "critical data and bringing operations there to a halt for several days" (Chan, 2016).	Not declared

Methodology

The study examines the data concerning the costs and losses caused by cybercrime that are available in literature and studies from the Gulf Corporation Council (GCC) countries and worldwide examining the valid causes of such harms. Additionally, the Social Insurance Organization of the Kingdom of Bahrain (SIO)[1] data shows that the total number of IT and IT-related workforce in Bahraini conventional and Islamic banks is 168. Therefore the entire population was selected for this study. Quantitative research method use and out of 168 self-administrated questionnaires 119 IT employees responded, and ten questionnaires were rejected because they were not completed.

Results and Discussion

- **Professional IT Security Certifications**

Table-02 illustrated that the majority of respondents do not have any specialized professional IT security certificates training course with 46. 9 %. Respondents have the fundamentals of cybersecurity certificate that is known as CompTIA Security+ for 9.2 %. In comparison, who has a Certified Information system manager, 9.2 % of them, and for the SANS GIAC Security Essentials 8.4 %. Respondents who have Certified Information System Security Professional for 7.6%, whereas only 2.3% of them have a certified Ethical Hacker. This is a clear sign of lack of interest in training courses that raise the level of awareness and progress in the field of rapid technical change.

Table-02 *Distribution of the respondents according to professional IT Security Certifications*

IT certification	Frequency	Percent
CompTIA Security+	12	9.20%
GSEC	11	8.40%
CISSP	10	7.60%
CISM	12	9.20%
CEH	3	2.30%
Other certificates	21	16%
No certification	61	46.90%

[1] https://www.sio.gov.bh/

- **Number of employees in the bank**

Participants were requested to report the number of employees in their banks to estimate the size of the bank. As shown in Table-03, banks are divided into six categories (from less than 100 employees, 100 to 199, 200 to 299, 300 to 399, 400 to 499, and 500 and more employees). Table-03 demonstrates the highest number of employees, 38.5%, in the bank were in the category of 300-399 employees. The lowest group was 6.4%, and they were between 400-499 employees, while 9.2% were for the group of fewer than 100 employees and 13.8% for the category of 100-199 employees. Meanwhile, 22% said that the number of employees is from 200 to 299, and only 10.1% of them indicated that the number of employees in their bank was 500 and above. This is an indication that the highest number of respondents of IT-related employees in the Bahraini banking sector is in the category of 300-399 employees.

Table-03 *Distribution of the respondents according to the total number of employees in the bank*

No of the employee in the bank	Frequency	Percentage
Less than 100	10	9.2%
100-199	15	13.8%
200-299	24	22%
300-399	42	38.5%
400-499	7	6.4%
500 and above	11	10.1%

- **No of employees in the IT department**

Participants were asked to report the number of IT employees in their IT department to estimate the size of the IT department in the bank. As shown in Table-04, the banks were divided into four categories (very small <5, average 5 to 10, medium 10-15, and large >15). Most of the participants belong to the large bank category at 52%, followed by small at 20%, then by average at 15%, and lastly medium at 13%. This is an indication that the highest number of IT-related employees is the Bahraini banking sector is in a large category of above 15 specialists.

Table-04 *Distribution of the respondents according to No of employees in your IT department*

No of the employee in the IT department	Frequency	Percentage
Less than 5	22	20%
5-10	16	15%
10-15	14	13%
More than 15	57	52%

4.3.2 General Information

- **The person responsible for information security in the organization**

Respondents were requested to report about the person responsible for the information security in the bank. Table-05 shows that the majority of respondents said that the information security is under the security manager's responsibility at 37.6%, while 25.7% of participants said that it is under the Chief Information Security Officer (CISO) responsibilities, and 21.1% said it is under IT managers, directors or Chief Information Officers (CIO). On the other hand, 7.3% of them said information security comes under security directors, whereas 1.8% are under a Chief Operating Officer (COO), and it is under the responsibility of other workers in the IT department for 6.4%. Brooks' (2017) study of 723 responses indicated that 65% of businesses do not have a dedicated person or department responsible for cybersecurity.

Table-05 *Distribution of the respondents according to who is responsible for information security in your organization*

Responsibility for Information security in your bank	Frequency	Percentage
CISO	28	25.7%
Security Manager	41	37.6%
IT Manager/ Director / CIO	23	21.1%
Security Director	8	7.3%
COO	2	1.8%
Other	7	6.4%

- **Bank's level of preparedness to respond to natural disasters**

Regarding the bank's level of readiness to respond to natural disasters, Table-06 show that of participants, at 94.5%, said that their banks were prepared. In comparison, 2.8% of the respondents said their banks were not ready to respond to natural disasters, and 2.8% do not know about this information. This is an indication that the majority of Bahraini banks were prepared for the natural disaster.

Table-06 *Banks level of preparedness to respond to natural disasters*

Level of preparedness	Frequency	Percentage
Prepared	103	94.50%
Not Prepared	3	2.80%
Do not know	3	2.80%

- **Security frameworks**

Respondents were asked to report the framework used in their bank. Table-07 demonstrates that most participants, 41.3% of the employees in the IT department, stated that their bank adheres to ISO/IEC27000, while 22.9% said that they followed Information Technology Infrastructure Library (ITIL). 21% of the participants declared that they followed the security management framework, and the same percentage said they followed the Payment Card Industry Data Security Standard (PCI DSS). 18.3% of them said that their banks never used any framework and/or standards. 11% of participants announced that they followed Control Objectives for Information and Related Technology framework (COBIT). At the same time, there are 6.4% who said that they use other frameworks or standards. In comparison, for the National Institute of Standards and Technology (NIST) 4.6% of respondents said their banks use it. This indicates that the majority of Bahraini banks adhere to ISO/IEC27000.

Table-07 *Distribution of the respondents according to cybersecurity frameworks*

Rank	Cybersecurity framework	Frequency	Percentage
1	ISO/IEC27000	45	41.3%
2	ITIL	25	22.9%
3	Security management	23	21.1%
3	PCI DSS	23	21.1%
5	No framework or standard	20	18.3%
6	COBIT	12	11.0%
7	Other	7	6.4%
8	NIST	5	4.6%

- **The priority of cybersecurity within the bank**

Participants were asked to indicate their opinion about the priority of the cybersecurity within their bank. Table-08 illustrated that 67.9% of participants stated that their banks place a high priority on cybersecurity, whereas 18.3% of them said that the priority of cybersecurity within their bank is moderate. The result was reached from 7.3% of participants that the priority of cybersecurity within their banks was low, but 6.4% were not sure about it. This is an indication that cybersecurity has a high priority in Bahraini banks.

Table-08 *Priority of the cybersecurity within the respondent's bank*

Cybersecurity priority within your bank	Frequency	Percentage
Low	8	7.3%
Moderate	20	18.3%
High	74	67.9%
Not sure	7	6.4%

- **The topic of cybersecurity presented or discussed at the bank executive leadership meeting**

Table-09 shows that the majority (almost 37%) of the respondents indicated that cybersecurity topics were presented or discussed at bank executives' meetings every month. While 24.8% of them said it is considered occasionally, followed by 22% of respondents who said quarterly and others, at 16.5%, indicated they discussed the issue every week.

Table-09 *Topic of cybersecurity presented or discussed at their executives' meetings*

Cybersecurity often discussed	Frequency	Percentage
Weekly	18	16.5%
Quarterly	24	22.0%
Monthly	40	36.7%
Occasionally	27	24.8%

- **Threats that have the most increased the risk exposure over the last 12 months**

As is shown in Table-10, malware comes in the first ranking of threats that have the most increased banks' risk exposure over the last 12 months, according to 60 responses of IT department employees in Bahraini banks, at 55%. The second-ranking is for spam, according to 53 responses at 48.6%, while phishing comes in the third-ranking, based on 44 responses at 40.4%. Fourth is the Distributed Denial-of-Service attack for 31 answers at 28.4%, after which comes fraud in the fifth rank for 29 replies at 26.6%. Sixth is data theft giving 26 answers at 23.9% after that is the internal attacks corresponding to 14 replies at 12.8%. Subsequently, the eighth ranking is for cyber-attack to steal IP and ransomware based on 12 answers at 11%. The tenth is zero-day attacks from 9 respondents at 8.3%. In contrast, natural disasters are in the eleventh ranking according to 5 responses at 4.6%, and espionage comes in the last rank for two responses at 1.8%. This is a clear indication of the strength of internal threats in Bahraini banks.

Table-10 *Ranking of threats that have most increased your risk exposure over the last 12 months*

Rank	Threats that have most increased your risk exposure over the previous 12 months	Frequency	Percentage
1	Malware	60	55%
2	Spam	53	48.6%
3	Phishing	44	40.4%
4	DDOS attack	31	28.4%
5	Fraud	29	26.6%
6	Data theft	26	23.9%
7	Internal attacks	14	12.8%
8	Cyber-attack to steal IP	12	11%
8	Ransomware	12	11%
9	Zero day attacks	9	8.3%
10	Natural Disaster	5	4.6%
11	Espionage	2	1.8%

- **Level of how knowledgeable are employees about their bank's security risks**

Table-11 presents how knowledgeable employees were about their Bahraini banks' security risks according to the opinions of IT department employee responses. Consequently, 13.8% stated that they are very knowledgeable about security risks. In comparison, 40.4% said they were knowledgeable, and the same percentage of 40.4% of responses were for somewhat knowledgeable, and 5.5% said that they were not knowledgeable about security risks. This indicates the need for the execution of security risk knowledge, awareness and training.

Table-11 *Distribution of the respondents according to how knowledgeable are employees about your organization's security risks*

Employee cybersecurity knowledge	Frequency	Percentage
Very Knowledgeable	15	13.8%
Knowledgeable	44	40.4%
Somewhat Knowledgeable	44	40.4%
Not Knowledgeable	6	5.5%

Regarding the impact of cyber-attacks in banks, the participant's response number ranking of the impact of cyber-attacks in banks , as is shown in Table-12. The first rank was reputational damage, which has the highest incidence of cyber-attacks in banks, with the bulk of respondents at 81.7%; the financial loss comes in the second-ranking of impacts, as stated by 77.1% of participants. The third-ranking was for customer information loss as indicated by 62.4% participants, followed by the disruption of the business process (ranked 4) with 59.6% responses after that was the theft of IP as the fifth ranking of cyber-attacks' impact on the banks, as stated by 49.5% of participants. The sixth ranking was for regulatory noncompliance impact, reported by 37.6%, whereas the seventh ranking was for effect on employee morale, indicated by 30.3% of respondents. The reputational damage is the highest impact of cyber-attacks in banks.

Table-12 Ranking of the impact of cyber-attacks in banks

Rank	Impact of Cyber-attacks in banks	Frequency	Percentage
1	Reputational damage	89	81.7
2	Financial Loss	84	77.1
3	Customer Information loss	68	62.4
4	Disruption of Business process	65	59.6
5	Theft of IP	54	49.5
6	Regulatory noncompliance	41	37.6
7	Effect on Employee morale	33	30.3

- Level of experience toward theft, corruption of corporate or user/consumer information

Table-13 demonstrates the level of knowledge of the theft, corruption of corporate, or user/consumer information. The table shows that 41.3% of respondents' indicated that threat was the source of external actors, while 17.4% stated that the source of the risks was from internal actors, and finally, 41.3% of them preferred to ignore or not to answer this question. This indicates the seriousness of threats from within the organization.

Table-13 *Distribution of the respondents according to experience the theft, corruption of corporate or user/consumer information*

Experienced theft, corruption	Frequency	Percentage
Internal threat actors	19	17.4%
External threat actors	45	41.3%
No answer	45	41.3%

Conclusion

The majority of respondents were Bahraini (72%) and between the ages of 30-39 years, working in the IT department in the banks. This indicates that most of the respondents to the questionnaire are Bahraini working in the IT department in the banks, with 61% carrying a BSc degree. This is an indication of the high level of education of the respondents working in IT departments in the banks. Furthermore, the majority of respondents do not have any specialized professional IT security certificates training course with 46.9%. This is a clear sign of lack of interest in training courses that raise the level of awareness and progress in the field of rapid technical change, or maybe there is no support from the top management to pursue professional certification in IT security. Nevertheless, the Bahraini Government, through TAMKEEN, is taking full responsibility for Bahraini to be internationally professionally IT qualified.

Regarding the bank's level of preparedness to respond to natural disasters, the majority of participants, with 94.5%, indicated that the Bahraini banks are prepared for natural disasters. Respondents were asked to report the framework used in their bank that most of the participants, with 41.3% stated that their bank adheres to ISO/IEC27000. This indicates that the majority of Bahraini banks subscribe to ISO/IEC27000.

Almost 68% of participants stated that their banks place a high priority on cybersecurity, and this is an indication that cybersecurity has a top priority in Bahraini banks. Malware comes in the first ranking of threats that have the most increased banks' risk exposure over the last 12 months, according to 55% of IT department employees in Bahraini banks. This is a clear indication of the strength of internal threats in Bahraini banks.

When the participants were asked how knowledgeable are about security risks, about 46% indicated that they are between somewhat knowledgeable to not knowledgeable. This indicates the need for the execution of security risk knowledge, awareness and training.

The board should play a significant role in driving the IT strategy, given its importance in corporate strategy. This should cover every dimension of the management of technology systems. That is to say: cost, human capital, hardware and software, vendors and service providers, and risk management, including disaster recovery, should be factored in the IT strategy of the bank. While the budget is the financial facility, which firstly rationally estimates the costs and secondly assesses the access to the resources required to achieve successful implementation of cybersecurity.

References

Al-Alawi, A, I., Yousif Al-Marzooqi, N., & Fraidoon Mohammed, Y. (2007). Organizational culture and knowledge sharing: critical success factors. *Journal of Knowledge Management*, *11*(2), 22-42.

Al-Alawi, A. I. (2006). Investigating the strategies for successful development of health information systems: A comparison study. Information Technology Journal, 5(4), 626-647.

Al-Alawi, A. I. (2014). Cybercrimes, Computer Forensics and their Impact in Business Climate: Bahrain Status. *Research Journal of Business Management*, *8*(3), 139-156.

Al-Alawi, A. I., & Al-Ali, F. M. (2015). Factors affecting E-commerce adoption in SMEs in GCC: an empirical study of Kuwait. *Research Journal of Information Technology*, 7(1), 1-21.

Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Evaluation of telecommunications regulatory practice in the Kingdom of Bahrain: development and challenges. *International Journal of Business Information Systems*, *31*(2), 282-303.

Al-Alawi, A. I., Al-Bassam, S. A., & Mehrotra, A. A. (2020a). Critical Cybersecurity Threats: Frontline Issues Faced by Bahraini Organizations. In *Implementing Computational Intelligence Techniques for Security Systems Design* (pp. 210-229). IGI Global.

Al-Alawi, A. I., Mehrotra, A. A., & Al-Bassam, S. A. (2020b). Cybersecurity: Cybercrime Prevention in Higher Learning Institutions. In *Implementing Computational Intelligence Techniques for Security Systems Design* (pp. 255-274). IGI Global.

Al-Alawi, A. I., Mehrotra, A. A., Elias, H., Safdar, H. S., & Al-Bassam, S. A. (2020). The Implications of Unethical and Illegal Behavior in the World of E-Commerce. In *Ethical Consumerism and Comparative Studies Across Different Cultures: Emerging Research and Opportunities* (pp. 152-230). IGI Global.

Al-Awadi, M., & Renaud, K. (2007, July). Success factors in information security implementation in organizations. In *IADIS International Conference e-Society*.

Al Awawdeh, S., & Tubaishat, A. (2014, April). An information security awareness program to address common security concerns in IT unit. In *Information Technology: New Generations (ITNG), 2014 11th International Conference on* (pp. 273-278). IEEE.

Arab News. (2015). Aramco foils $30 million scam. [Online], Retrieved March 3, 2017, from http://www.arabnews.com/saudi-arabia/news/823001

Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. *Journal of Library Administration*, *54*(1), 46-56.

Armencheva, I., & Smolenov, S. (2015). FROM REAL CYBER CONFLICT THROUGH WISHFUL CYBER SECURITY TO (UN) LIKELY CYBER PEACE. *Land Forces Academy Review*, *20*(3), 259-266.

Axelrod, R., & Iliev, R. (2014). Timing of cyber conflict. *Proceedings of the National Academy of Sciences*, *111*(4), 1298-1303.

Bertram, M., & Waters, C. (2016). How to Avoid Repeating History in ITS Security. Atkins, 1st edition, February 2016, Access February 2018. http://northamerica.atkinsglobal.com/~/media/Files/A/Atkins-Corporate/north-america/documents/How2AvoidRepeatingHistory_20160224.pdf

Chan, S (2016), Cyberattacks Strike Saudi Arabia, Harming Aviation Agency, *New York Times*, Retrieved January 2017, https://www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html

Ghorsad, T. (2014). Perceiving Cybercrime – Appearance, Challenges and Legal Reaction. *International Journal of Research*, 1(6), 626-634.

Government, HM. (2015). Small Businesses: What you need to know about cybersecurity [online], [Retrieved March 12, 2015] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/412017/BIS-15-147-small-businesses-cyber-guide-March-2015.pdf.

Kaspersky (2018), The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Retrieved February 26, 2018. https://www.kaspersky.com/blog/the-human-factor-in-it-security/

Ma, Q., Schmidt, M. B., & Pearson, J. M. (2009). An integrated framework for information security management. *Review of Business*, 30(1), 58–69.

Maggio, G., & Cacciola, G. (2012). When will oil, natural gas, and coal peak?. *Fuel*, *98*, 111-123

Metzger, M (2015), Hacker Buba' holds UAE bank to ransom, *SC Media Magazine,* Retrieved January 2018, https://www.scmagazineuk.com/hacker-buba-holds-uae-bank-to-ransom/article/535548/

Morgan, S. (2016, January 30). *Why J.P. Morgan Chase & Co. Is Spending A Half Billion Dollars On Cybersecurity. Forbes.* Retrieved from http://www.forbes.com/sites/stevemorgan/2016/01/30/why-j-p-morgan-chase-co-is-spending-a-half-billion-dollars-on-cybersecurity/#721ada9c2a7f

Perlroth, N. (2012). Cyberattack on Saudi Firm, US sees Iran firing back. *New York Times*, *23*.

Ponemon Institute (2015), “2015 cost of Cyber Crime Study: Global”, Sponsored by Hewlett Packard Enterprise, Independently conducted by Ponemon Institute

LLC, Publication Date: October 2015. [Online], [Retrieved May20, 2016] http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf.

Ponemon Institute (2014), “2014 Cost of Cyber Crime Study: United States,” 30October2015. [Online], [Retrieved August, 2016]. www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime.

Ponemon Institute (2017),” 2017 Cost of Data Breach Study: Global Overview Benchmark research” sponsored by IBM Security, Independently conducted by Ponemon Institute LLC, Publication Date: June 2017. [Online], [Retrieved September 2017]. https://www.ibm.com/security/data-breach

PWC (2015). Managing cyber risks in an interconnected world
Key findings from The Global State of Information Security® Survey 2015. PricewaterhouseCoopers. Retrieved from
http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

Reuters (2013). "Six Arrested in $45 Million Global Cybercrime Scheme." Reuters. Thomson Reuters, 18 Nov. 2013. Retrieved January 2018. www.reuters.com

Security Middle East (2015). Cybercrime one of the biggest Middle East security threats. (2015, January 05). Retrieved February 21, 2018, from http://securitymiddleeast.com/2015/01/05/cybercrime-one-biggest-middle-east-security-threats/

SEL (2015), SEL Cybersecurity Solutions, Defense-in-depth cybersecurity that mitigates threats with sustainable, proactive solutions. Schweitzer Engineering Laboratories, Inc. [online], [Retrieved April, 12, 2016]. https://cdn.selinc.com//assets/Literature/Product%20Literature/Flyers/PF00250_CybersecuritySolutions_20151013_Pubs.pdf?v=20151105-140235.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. Oxford University Press.

Tahoun, E. A., & Maklad, J. (2015, May 23). Why Is It Urgent to Deter Cybercrime In the Middle East?. Retrieved February 21, 2018, from https://www.researchgate.net/publication/317648264_Cyber_Crime_in_the_Middle_East_Analysis

Thomas, K (2015), Hacker Buba releases data belonging to customers of a UAE bank, *We Live Security News. Retrieved* January 2018, https://www.welivesecurity.com/author/karlthomas/