Journal of International Women's Studies

Volume 25 | Issue 1 Article 21

February 2023

Women in Cybersecurity: A Study of the Digital Banking Sector in Bahrain

Adel Ismail Al-Alawi
Professor, Management & Information System, College of Business Administration, University of Bahrain, Kingdom of Bahrain.

Noora Ahmed Al-Khaja
Engineering Management Program, College of Civil Engineering, University of Bahrain, Kingdom of Bahrain

Arpita Anshu Mehrotra
Head of Department, College of Business and Financial Sciences, Royal University for Women, Kingdom of Bahrain

Women in Cybersecurity: A Study of the Digital Banking Sector in Bahrain

By Adel Ismail Al-Alawi,[1] Noora Ahmed Al-Khaja,[2] and Arpita Anshu Mehrotra[3]

Abstract

Cybersecurity is of utmost importance due to the sophisticated cyber-attacks occurring, mainly in the banking sector. Cybersecurity is considered a vital industry to protect and secure both the consumer and the owner. This study aims to examine and investigate women in the field of cybersecurity in the digitized banking sector. This study covers several factors that affect women's contributions in this field, including challenges and limitations, women in Fintech and ecosystem, women involved in digital transformation, women in applying cybersecurity management strategy, social and economic impacts, and skills and qualifications in the field of cybersecurity for banking. Most of the studies highlight the shortage of women in this field and the need for improvement and innovation. Quantitative and qualitative methods were conducted to ensure the credibility of the information provided. The results illustrate that women in Bahrain can work successfully in the cybersecurity field and overcome the challenges and limitations. Moreover, women are interested in advancing in this field and promoting their skills in improving cybersecurity in the digitized banking sector. Most of the previous studies have mainly focused on women joining the cybersecurity field, but they have not sufficiently addressed their role and importance in the banking sector, which is considered one of the most important sectors requiring cybersecurity. The study results recommend that the government of Bahrain and organizations can positively impact women's progress in this field through encouragement and incentives, which will eventually lead to the economy's growth in Bahrain. Furthermore, women's awareness of the cybersecurity field as a career option should be increased through training sessions and opportunities to achieve professional qualifications and certifications.

Keywords: Cybersecurity, Digitalization, Banking, Women, Fintech and Fintech ecosystem, Management strategy, Bahrain

Introduction

Information and Communication Technology has transformed the world and has created newer opportunities for the global economy and humanity. However, the world is exposed to new vulnerabilities and many cyber activities by a range of hackers and criminals, which leads to the need for and importance of cybersecurity (Callen-Naviglia & James, 2018). Cybersecurity is defined as all activities and measures intended to prevent and cover any attacks focusing on information systems connected to cyberspace (Zahout, 2017).

The past records and the present status show that a minority of women are engaged in cybersecurity as many obstacles hinder their progress in this field. Involvement in cybersecurity

[1] Professor, Management & Information System, College of Business Administration, University of Bahrain, Kingdom of Bahrain. Email: adel.alalawi@gmail.com.

[2] Engineering Management Program, College of Civil Engineering, University of Bahrain, Kingdom of Bahrain. Email: n.alkhaja@live.com.

[3] Head of Department, College of Business and Financial Sciences, Royal University for Women, Kingdom of Bahrain. Email: amehrotra@ruw.edu.bh.

depends on one's interest in Science, Technology, Engineering, and Math (STEM) (Shumba et al., 2013, Al-Alawi et al., 2019). Cybersecurity is of critical importance, and the market labor of this sector has been undergoing numerous changes over the years. Cybersecurity is needed in the dynamic digitized banking sector. The professionals in this field have been suffering from a shortage of capable workforce over the years, and women workers can help to fill the gap. More women are needed in this field as only 11 percent of cybersecurity positions were held by women as of 2018 (Fernandes, 2018).

Statement of the Problem

The lack of women's involvement in cybersecurity in the banking sector in Bahrain is due to the persistent challenges women face and the risks associated with this field. However, cybersecurity strategy plays a vital role in the innovative banking sector, which is considered very important in today's world due to the advancement of technology and the digital transformation taking place in banking systems.

Study Questions

The present study seeks to address the following questions:

- What are the challenges and barriers that prevent women from succeeding in the career of cybersecurity strategy?
- What will be the contribution and role of women in cybersecurity in the banking sector?
- What is the importance of women's contributions in the Fintech and Fintech ecosystem, digital and digital transformation, and management strategy in banking cybersecurity?
- What is the economic and social impact of women's participation in the cybersecurity field?
- What are the skills required for women to succeed in the field of cybersecurity strategy?
- Are women in the banking sector qualified with the Information Systems Audit and Control Association (ISACA) qualifications or any other type of certification related to cybersecurity?

Objectives of the Study

- Investigate the challenges and limitations hindering the advancement of women's careers in cybersecurity strategy
- Examine the role and contribution of women in the cybersecurity innovative banking sector
- Illustrate women's impact in the Fintech and Fintech ecosystem, digital and digital transformation, and cybersecurity management strategy sectors within the banking industry
- Study the economic and social impact of women in cybersecurity
- Examine the skills and qualifications required for women to succeed in cybersecurity strategy

Study Limitations

This study will focus on women in cybersecurity through the digitized banking sector that will be limited to cybersecurity, banking, and Bahrain's Kingdom. There were some limitations in

the data collection as the number of specialized experts in this field in the Kingdom of Bahrain is limited. Approximately half of the respondents in the study were men, and half women. However, the number of women in the field keeps increasing due to the need for knowledge in this field. This had been a lesson learned from the COVID-19 pandemic.

Study Structure

This study is divided into five main sections. The first section sets the background of the research and articulates the aims of this study. Following this, the second section briefly summarizes the literature review conducted on women in cybersecurity in the banking sector. The third section discusses the methodology of quantitative and qualitative methods conducted through questionnaires and interviews, followed by the study design and framework. The findings and analysis are elaborated in the fourth section. The final section sums up the study's findings and provides recommendations that will help formulate efficient policies and assist in future studies.

Literature Review

This section highlights the previous studies relating to eight factors that affect women's contributions to cybersecurity in the banking sector. These factors are women's challenges and limitations, women's contribution and role in the banking sector, women in Fintech and Fintech ecosystem, women in digitization and digital transformation, women in applying cybersecurity management strategy, social and economic impacts, women's skills and qualifications.

Challenges and Limitations Faced by Women in Cybersecurity

Women face various challenges and hindrances in the field of cybersecurity. However, the two main barriers to advancing in a cybersecurity career are social and personal barriers (Bagchi-Sen et al., 2010).

The social barrier refers to women who might be socially isolated or separated from the information technology field, unlike men who are considered experts, especially as they are more familiar with the hacking field. In addition, the cybersecurity field could demand late nights in computer laboratories. Even working during the weekend could be a requirement for the job profile, which many patriarchal cultures might not accept for women, as such work could affect their safety, reputation, and time spent on family matters. The patriarchal culture of Bahrain contributes to the predominance of men in this field. Developing skills through higher education in computer science may lead to an increase in women's participation in this field. However, the reality is that women working in this field, particularly married women, may face more difficulties in order to balance work with their domestic responsibilities at home, which are often less of a burden for men (Bagchi-Sen et al., 2010, Al-Alawi, et al., 2021).

The second barrier revolves around education, personal characteristics, and personal interests as shaped by culture. In information technology, most people obsessed with such technology are considered "nerds" since they like to work with complicated IT systems, and these characteristics are stereotypically assigned to men rather than women. Entering into the cybersecurity profession requires expertise in different fields such as mathematics, science, engineering, and being a decision-maker. In addition, to succeed in this field, several criteria must be met, such as a solid technical background in these fields and the willingness to use knowledge to suggest changes to laws and regulations (Bagchi-Sen et al., 2010).

Shumba et al (2013) have studied cybersecurity professionals and surveyed women's barriers in this field. Some of the obstacles they identified included: women's lack of awareness

of the cybersecurity field; lack of encouragement from family and community; the structure of the courses appealing to male interests; and the belief that cybersecurity is a future career for people holding degrees in computer science and information technology, degrees which restrict the entry of women into this field.

Poster (2018) illustrates that women comprise only 11 percent of cybersecurity professionals worldwide and only 14 percent in North America. In addition, women make up 57 percent of the United States' professional workforce in this field. At the same time, this year, it is estimated that two million more cybersecurity jobs will be needed worldwide. Furthermore, out of the 3.2 million people already employed in the field, almost 750,000 are in the United States. This study illustrates the global need for women in cybersecurity. Based on the previous arguments, it is hypothesized that:

> H_1: Women face a lot of challenges and limitations in pursuing a career in the cybersecurity digitized banking sector.

Women's Contribution and Role in the Banking Sector

Banks have recognized that the best method of empowering the banking systems is digital finance and providing access to finance. It is considered a central issue that is important for the empowerment of women. A study conducted in Nigeria illustrated the fact that 40.9 percent of Nigerian women have no bank account compared to 32.5 percent of men. Women have customarily been excluded from the external information domain, often deliberately due to factors like lack of freedom of movement or low levels of education (Ugwuja et al., 2019).

The career progression in this field shows that some barriers should be eliminated for both genders in the financial field. However, women form a minority in the top management of the financial sector. The opportunities and solutions for the future have increased the possibility of women being promoted in top management positions and removing the obstacles that interfere with their career advancement. A survey conducted in the United Kingdom in the banking sector shows that culture and organizations are the two main barriers preventing women from achieving roles as top management in the financial industry. Even though there are around 528,000 employees in the United Kingdom's financial sector except for two departments of insurance and pensions, only 90,000 of these are women, representing only 30 percent (Al-Alawi, 2016).

Women have access to the outside world through digital finance. Digital finance conducted through Information and Communications Technology (ICT) allows the users greater financial inclusion. The financial service sector is a primary driver of communications and network technology. There are many digital financial services offered that include: fund transfers; mobile finance systems for payments; micro-lending platforms; notification systems for clients; savings; client enrolment through SMS; micro-insurance products, including life and weather index insurance; claims payment through mobile phones; and analysis of loans in the field using smartphones (Ugwuja et al., 2019).

Cyberattacks can be detrimental for consumers and banks as many cybercriminals find loopholes and develop sophisticated methods of attacking the weaknesses in the banking systems. Due to technological capabilities, various methods of attacking and damaging are spreading, which target the banking sector. This has led the banks to be cautious of the threats and challenges ahead and to adopt proactive security (Ugwuja et al., 2019). Considering this, we hypothesize that:

H_2: Women's increased participation and contributions will significantly impact the cybersecurity digitized banking sector.

Women in Fintech and Fintech Ecosystem

Women face more significant barriers than men in accessing the finance world. Women who own their firms face lots of rejection even though they have a secure banking relationship. Based on a study that was conducted, two policies were suggested. The first policy indicated that there should be an effort to facilitate and incorporate the companies owned by women to help the gender target in this field. The second policy revolves around encouraging the banks to lend businesswomen. Lending practices will help women facing difficulties in this field by considering the collateral deposits and credit assessments that these firms are suffering to resolve. One of the most effective policies could be to reconsider the credit assessment process, which will significantly increase the standard practices done through the Fintech space (DiCaprio et al., 2017). Based on the previous argument, the following hypothesis can be formulated:

H_3: More women in Fintech and Fintech ecosystem will positively impact the development of the cybersecurity digitized banking sector.

Women in Digitalization and Digital Transformation

Digitalization in the banking sector is one of the primary methods to keep banks competitive. A study by Malmström & Wincent (2018) on women applying for loans versus men showed that women do not get access to capital quickly. Even if they get approval for the finance they requested, they need to fulfill more demands on credit terms than men. The reality of this discriminatory action comes from gender stereotyping as banks consider men to be more ambitious and to have more potential and capabilities than women. Unfortunately, gender stereotyping plays a persistent role in the finance world. Considering this, we hypothesize that:

H_4: Women trained in digitalization and digital transformations will have a positive impact on the cybersecurity digitalized banking sector.

Women in Cybersecurity Management Strategy

The main objective of the cybersecurity management strategy is to reduce the number of cyber-attacks and threats. Governments usually adopt many e-services that require security and high safety measures against any threats ahead (Giri, 2019).

Women in cybersecurity, unfortunately, are considered to have a minor and limited representation in this field. Many women in the field feel like outsiders, but this will hopefully change in the near future as women gain the necessary education, compete with men for leadership positions, and apply cybersecurity strategies through their tasks (Al-Alawi, 2016; Lingelbach, 2018). As a result, we have developed H_5:

H_5: Increased opportunities for women in cybersecurity management will have a positive impact on the digitalized banking sector.

Economic and Social Impacts of Women's Increased Participation

Women joining the field of cybersecurity will have more confidence and self-efficacy. In addition, career and research opportunities will be multifold for them by engaging in this field and will add another dimension to the social identity of women in these careers (Rowland et al., 2018).

Women's cybersecurity awareness and knowledge will have a significant impact on the business world's advanced protection. This awareness will be reflected as an amendment program for society and will be a turning point for women's success in management and leadership positions in the banking sector (Chelly, 2016; Al-Alawi, 2016). It leads to the hypothesis that:

> H_6: Women's increased participation in the cybersecurity digitalized banking sector will have positive economic and social impacts on women, the field, and the larger society.

Women's Skill Development

If women get the required encouragement to participate in the cybersecurity field, this would undoubtedly boost the number of skilled professionals into the cybersecurity industry. A vibrant cybersecurity industry helps protect businesses overall. Furthermore, addressing the gender gap would create an innovative, collaborative environment and strengthen communication. As a result, growth of the cybersecurity banking sector could be achieved. An excellent way to motivate women in this field is by allowing them to capitalize on their skills, which would increase the financial sector's opportunities and help in its growth. According to Deen (2019), encouraging women to join the cybersecurity field will generate more women with technical talents in the IT domain.

Further, Deen's study stated that during the year 2018, Information Technology spent US$101 billion and that figure was expected to rise about 35% in the next three years. These figures suggest many opportunities and openings for women pursuing secure employment and competitive salaries in the IT sphere. Additionally, it was indicated that women studying STEM-related disciplines have to be encouraged to consider a career in cybersecurity.

According to research related to women's skills, studies show that the quality of self-efficacy is essential for women in the process of career selection and in their progression in the cybersecurity field. Unfortunately, the lack of women's interest in STEM lowers their self-efficacy (Malmström & Wincent, 2018). Consequently, we predict that:

> H_7: The greater the technical, communication, and people skills of women, the more success they can achieve in the field of the cybersecurity digitalized banking sector.

Women's Qualifications

The continuous technological advancement of cybersecurity has required the need for qualifications in cybersecurity. To be certified is a way of confirming that a person has the requisite knowledge and appropriate skills to enter the cybersecurity field (James & Callen, 2018).

In the Kingdom of Bahrain, there are 19 women and 240 men out of 259 active members in the Information Systems Audit and Control Association (ISACA) Bahrain Chapter. The 19 women had received the Certified Information System Auditor certification (CISA). Out of these 19 women, one is Certified in Risk and Information Systems Control (CRISC), and one has a Certified Information Security Manager certification (CISM) (interview with ISACA Board Members, Bahrain Chapter, personal communication, May 29, 2020). Consequently, we predict that:

H_8: Women are increasing their cybersecurity qualifications in the cybersecurity digitalized banking sector.

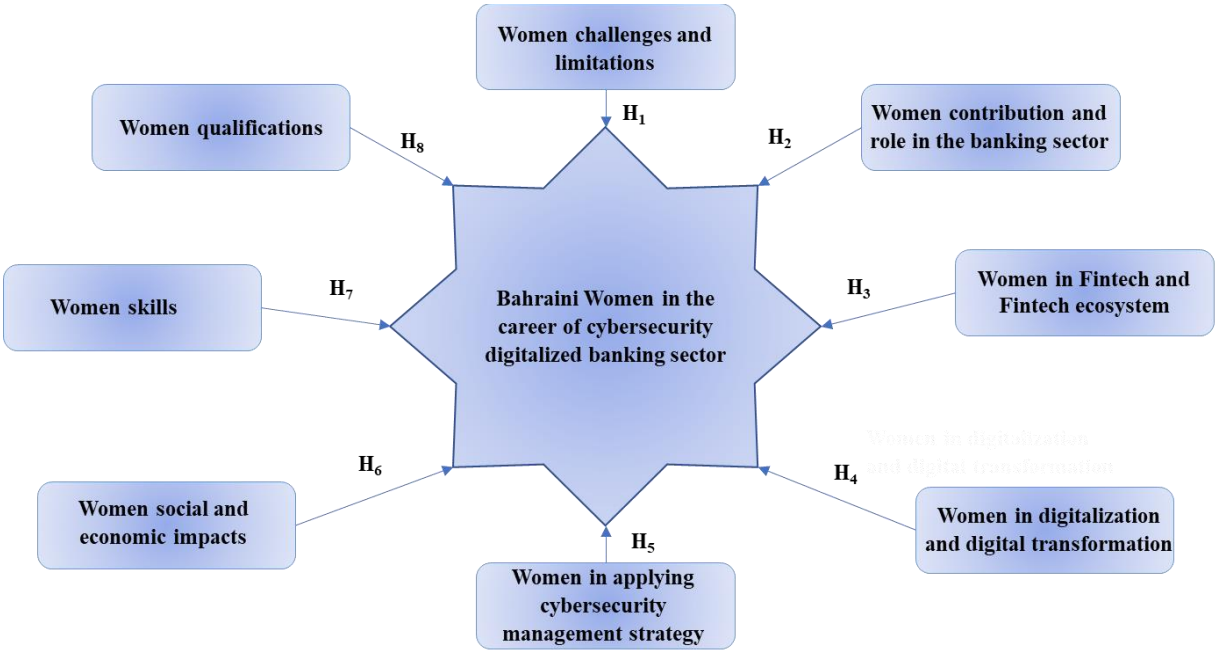
Study Methodology

Introduction and Framework

This study focuses on women in cybersecurity through the digitalized banking sector by examining several factors: challenges and limitations, women's role and contribution in the banking sector, women in Fintech and Fintech ecosystem, women in digitalization and digital transformation, women in applying cybersecurity management strategy, social and economic impacts of this career choice upon women, women's skills, and women certifications and qualifications in the field of cybersecurity in the banking sector. Both quantitative and qualitative methods were used to examine these factors.

The study framework revolves around how the several factors mentioned in the initial section of the methodology impact women in cybersecurity through the innovative banking sector. Figure 1 illustrates the conceptual framework of the factors affecting Bahraini women in cybersecurity through the digitalized banking sector.

Figure 1: The Conceptual Framework of the Factors Affecting Bahraini Women in Cybersecurity through the Digitalized Banking Sector



Study Design

The study consists of both quantitative and qualitative methods. The quantitative method was conducted through an online survey that was supported by using google forms. The questionnaire design had been completed after reviewing several questionnaires that have similar concepts to this research, such as Al-Alawi & Al-Bassam (2021). The factors that affect women in this field have been measured using the Likert Scale, where 1 represents strongly disagree, 2 disagree, 3 neutral, 4 agree, and 5 strongly agree. Furthermore, the Statistical Package for the Social Sciences (SPSS) was used for the descriptive statistics and the reliability test. The

questionnaire targeted employees who were in the fields of cybersecurity or banking in general. The qualitative method was conducted by interviewing some of the top ICT managers in the banking sector. The interviews were conducted virtually due to COVID-19 circumstances.

Data Analysis and Findings: Quantitative Questionnaire

This section aims to analyze the data conducted using the questionnaire. SPSS was used for analysis purposes to get the descriptive statistics and the reliability test to understand the essence of the methods and interviews. The questionnaire was sent as a google form link to approximately 75 participants in the field of cybersecurity, engineering, and top management in banks, and 50 participants responded. The questionnaire is divided into two main sections, personal data and organizational data.

Personal and Organizational Data

Of the 50 people in the survey group, 52% (26) were female, while 48% (24) were male. Although there is a minor difference in the percentage here, it is nonetheless significant given how much fewer women work in this field overall. The strong participation of women in our survey might be due to the fact that the survey was highly relevant for their own concerns, and they are greatly interested in cybersecurity in the banking sector.

There was a variety in the respondents' range of ages; those below age 25 were about 12%. The majority of the responses (32%) were between the ages of 26 and 30, 30% were 31 to 35 years old, the minority percentages of 4% were between 36 to 40 years old, and 8% were between the age of 41 and 45, while the last 14% were between the age of 46 years old and above. The women participants in the study, however, were significantly younger than the male participants (69% of the women were under 30, and only 6% were over 35), which suggests the existence of recent social changes allowing more women to participate in the field.

As for marital status, 54% overall were married, while 46% were single. Yet the percentages were quite different for women versus men. Whereas 16 of the 26 women were single (61.5%), only 7 of the 24 men were single (29%). 38% of the women in the study were married, so marriage and the huge family responsibility might also affect women's contribution in this field. The younger age of the women in the survey might also correlate to their higher likelihood of being single.

The nationality of 84% was Bahraini, and the rest of 16% were non-Bahraini. Questionnaires were conducted in the Kingdom of Bahrain. Out of 26 women in the study, only 3 were non-Bahraini. This shows that Bahraini women are interested in participating in this field.

Since education is the building block of any nation, the respondents' education level is important. In this survey group, the majority of 56% held a Bachelor's degree, 32% had a Master's degree, 6% had earned a Ph.D, 2% were Ph.D. students, and 4% were from the medical field. Comparing women and men, 36% of the women in the study had more than a Bachelor’s degree, whereas 54% of the men had more than a Bachelor’s degree (most often an MSc). However, 3 women were PhDs (or PhD students) compared to only 1 man. Overall, the data shows the capability and eagerness of Bahraini women for education and their desire to seek development and learning. The specialty of the survey respondents’ education was very similar for women and men. The main specialty was engineering, as that accounted for 48%. Participants from the business field were around 36%, with 4% each in Science and IT, and other specialists in computer science and medicine were 12%. Since the higher percentage of respondents were engineers, this

reflects that computer engineering and engineering majors are interested in this field as they are the core of cybersecurity.

As for their job status, overall 62% were employees, 20% were managers, 10% were supervisors, and 8% were head-of-road design group, retired, and students. There were significant gender differences here, as 85% of the women were employees, whereas only 37.5% of the men were employees. Men in the survey were much more likely to be managers and supervisors. In regard to the participants' years of experience, the majority of the survey respondents (58%) had fewer than ten years of experience, 26% had around 10 to 20 years of experience, 6% had 21 to 30 years of experience, and 10% had 31 or more years of experience. The vast majority of the women (80%) had under 10 years of experience, since they are comparatively younger than the male respondents in the study.

For questions about who was responsible for information security at their workplace, 60% of responses were IT manager, IT director, and chief information officer (C.I.O.). In comparison, 24% of the respondents identified that the chief information security officers (CISO) were responsible for cybersecurity, 8% said that the security director held this responsibility, and the rest of 8% noted other categories that branch into IT computer technical services and professors. Most (75%) of the men and about half (46%) of the women were IT managers, directors or CIOs.

Factors that Affect Women in Cybersecurity through the Digitalized Banking Sector

Factor 1: Women's Challenges and Limitations

Table 1: Women's Challenges and Limitations–Statements and Results

Statements	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Mean
Women's social life is a barrier to women's success in cybersecurity in the banking sector.	32%	22%	24%	20%	2%	2.380
Women lack knowledge of how to use the technology practically.	44%	14%	20%	18%	4%	2.240
Women have no interest in using and learning cybersecurity strategies.	38%	14%	14%	28%	6%	2.500
The culture encourages women to work in this field.	4%	16%	48%	28%	4%	3.120

Women's challenges and limitations are the main factors that affect women's introduction to cybersecurity in the banking sector based on the studies elucidated in the literature review. The four criteria to address the women's challenges and limitations were as per Table 1. The results show that more than half of the respondents (32% strongly disagree and 22% disagree) do not see women's social life as an obstacle towards achieving a career in cybersecurity through the digitalized banking sector. However, there were some disagreements between the men and women

in the study on this question. 30% of the women agreed that women's social life was an obstacle to a career in the field, compared to only 12.5% of men who either agreed or strongly agreed with that statement. The women's opinions regarding this statement may be given stronger weight since they have more direct knowledge of the experience.

Most disagree (44% strongly disagree, 14% disagree) that women lack knowledge regarding using the technology. Hence, we can conclude that women are aware and can use such technology and compete with males in career advancement.

Women show that they are interested in using technology and learning about cybersecurity in the banking sector by adopting new technologies, as illustrated by the results that 38% strongly disagree and 14% disagree that women have no interest in cybersecurity strategies. So, 52% are stating women's willingness to participate and seek knowledge in this field.

The culture could still be a barrier that women need to address to work in the field of cybersecurity since cybersecurity jobs might require a night shift, and the culture in the Kingdom of Bahrain, as in most of the gulf countries, is not conducive to women working in such fields. Yet 48% of responses in this study were neutral, illustrating that almost half of the respondents stated that the culture does not differ between males and females. Around 32% (28% & 4%) respectively agree and strongly agree that in the Kingdom of Bahrain, the culture encourages women to work in this field.

H_1: Women *may still face some* challenges and limitations in pursuing a career in the cybersecurity digitalized banking sector

Factor 2: Women's Contribution and Role in Cybersecurity in the Banking Sector

Table 2: Women's Contribution and Role in Cybersecurity in Banking Sector– Statements and Results

Statements	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Mean
Women will be promoted to management and cybersecurity leadership positions in banks.	2%	4%	30%	40%	24%	3.800
The development and growth of cybersecurity in the banking sector will be due to women's contribution.	2%	14%	46%	22%	16%	3.360

Table 2 illustrates that most respondents agree (24% strongly agree and 40% agree) that women's participation in the digitalized banking sector's cybersecurity will lead her to be promoted to management and leadership positions in the financial sector. In comparison, 30% opine that men and women will be treated equally in promotions. A minor percentage disagree (2% strongly

disagree and 4% disagree) that women might not be promoted to higher positions even though they will have significant contributions and roles in this field. The mean of the responses is 3.800.

The majority of 46% stated that this field's growth and development would be due in equal parts to men and women. In comparison, 22% agree and 16% strongly agree with the statement that women's contribution will lead to development and growth due to their innovation in this field.

H_2: Women's increased participation and contributions will significantly impact the cybersecurity digitized banking sector.

Factor 3: Women in Fintech and Fintech Ecosystem

Table 3: Women in Fintech and Fintech Ecosystem–Statements and Results

Statements	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Mean
Women's participation will improve the financial technology and process while using the banking system.	0%	6%	26%	36%	32%	3.940
Women's focus on cybersecurity jobs will increase security in financial technology.	0%	2%	36%	32%	30%	3.900
Women's cultural characteristics[4] might increase the performance of the banking payment system.	12%	16%	24%	24%	24%	3.320

Table 3 shows women in Fintech and Fintech ecosystem statements and results. Since the world is moving forward towards financial technology, around 68% (36% & 32% respectively) agree and strongly agree that women's role in financial technology will improve the process in the banking system through adopting new technologies in the financial sector.

Aiming to improve women's participation in Fintech and Fintech ecosystem will increase security in the banking sector. Almost 30% strongly agree, and 32% agree, indicating that women are on the right track to contribute to the banking sector's financial technology. In comparison, 30% are neutral that both men and women should focus on security jobs. A minor percentage of 2% disagree.

[4] Cultural characteristics might include communication differences, such as women being more talkative and social with customers and men getting straight to the point.

In response to the statement that women's characteristics and habits might increase the banking system's performance while performing their tasks, 24% of respondents strongly agreed, 24% agreed, and 24% were neutral. Hence, the majority of respondents believed that women's cultural characteristics might positively affect the performance of tasks in the banking sector. Simultaneously, a significant minority of 12% percent strongly disagreed and 16% disagreed with the statement that women's characteristics might increase performance of the banking payment system.

H_3: More women in Fintech and Fintech ecosystem will positively impact the cybersecurity digitalized banking sector's development.

Women in Digitalization and Digital Transformation

Table 4: Women in Digitalization and Digital Transformation– Statements and Results

Statements	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Mean
Women's ability to understand digitalization is high.	2%	2%	30%	38%	28%	3.880
Women working in digital transformation will reduce the number of errors.	4%	2%	38%	20%	36%	3.820
Women working in banks are aware of financial technology regulations that are used in the digitalized banking system.	4%	4%	30%	40%	22%	3.720

Table 4 shows the results of the survey about women in digitalization and digital transformation. These days most of the transactions in the financial sector in the Kingdom of Bahrain depend on digitalization to compete with other countries. More than half of the respondents believed that women could understand the digitalization process at a high level. Women can compete with men in adopting the digitalized tasks, since 38% agreed and 28% strongly agreed with this statement. The mean of this statement was about 3.880.

The number of errors will decrease through digital transformation. More than half of the percentage accepted this statement since 36% strongly agreed and 20% agreed. Hence, the respondents do not believe that women are the reason behind the errors since any human could commit mistakes. 38 percent gave a neutral response, reflecting that they see both men and women as part of the process of reducing errors by applying the digital transformation.

It seems that women working in the banking sector are aware of the digitalized banking system's regulations, as 22% strongly agreed with this statement, along with 40% who agreed. Hence, women’s level of awareness about regulations is high in the financial sector. The neutral responses were about 30%, believing that men and women are equal in awareness of regulations. Out of the minority percentage of 8%, 4% strongly disagreed and 4% disagreed that women are aware of the banks' digitalized systems.

H_4: Women trained in digitalization and digital transformations will have a positive impact on the cybersecurity digitalized banking sector.

Women in Cybersecurity Management Strategy

Table 5: Women in Cybersecurity Management Strategy– Statements and Results

Statements	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Mean
The ability of women to comply with and apply cybersecurity management strategies is high.	4%	18%	38%	26%	14%	3.280
Women will introduce and adopt new ideas for the cybersecurity management strategy.	0%	6%	26%	42%	26%	3.880

Table 5 illustrates the results for statements about women in cybersecurity management strategy. The ability of women to apply and comply with cybersecurity management strategies is considered high among the 26% who agreed and 14% who strongly agreed with this statement. In comparison, 38% are neutral, so in their opinion, men and women are equal in complying with and applying cybersecurity management strategies in the banking sector.

More than half of the total percentage showed a positive reaction to the statement that women will innovate in cybersecurity management strategy within the banking sector, as 42% agreed and 26% strongly agreed. This indicates that many believe women have creativity that will help them introduce new ideas for adoption in the field. In contrast, only a minor percentage of 6% disagreed with this statement as they believe that women cannot innovate in the cybersecurity management strategy. The high mean (3.880) also reflects confidence in women's creative abilities.

H_5: Increased opportunities for women in cybersecurity management will have a positive impact on the digitalized banking sector.

Economic and Social Impacts of Women's Increased Participation

Table 6: Economic and Social Impacts of Women's Increased Participation–Statements and Results

Statements	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Mean
Women's cybersecurity jobs in the banking sector will increase.	0%	14%	32%	22%	32%	3.720
Economic growth will rise due to women's contribution.	2%	12%	16%	44%	26%	3.800
Women's self-esteem, confidence, and motivation in the cybersecurity field will increase.	2%	0%	30%	36%	32%	3.960
Cultural barriers towards women will be removed.	4%	8%	20%	38%	30%	3.820

Table 6 shows the statements and results related to economic and social impacts of women's participation upon themselves and the wider economy and culture. Bahraini women's contribution in the field of cybersecurity in the banking sector will undoubtedly have an impact upon both the economy and society. From the economic perspective, the number of women working in this field will likely increase based on 22% who agreed and 32% who strongly agreed. However, 32% were neutral and 14% believed that the number of women in the field would stay the same. Around 66% believed that there would be a positive impact on the growth of the economy due to women's contribution in this field (44% agreed and 26% strongly agreed), so this suggests confidence that women's contributions will have a significant impact on the growth of the economy.

Most (68%) of the respondents agreed (36% agreeing and 32% strongly agreeing) that women's self-esteem, confidence, and motivation would grow within the cybersecurity field. This indicates that positive impacts are expected not only on the field itself, but also on the women involved.

The increased participation of women in cybersecurity will help women to be partners with men in this field. Culture might be an obstacle towards achieving women's dreams and goals, but 68% of the respondents believed that these cultural barriers towards women's career advancement in the Kingdom of Bahrain would be removed. The pessimists of the group (4% who strongly disagreed and 8% who disagreed) believed that the cultural barrier wouldn't be removed for women as mentalities are hard to change.

H_6: Women's increased participation in the cybersecurity digitalized banking sector will have positive economic and social impacts on women, the field, and the larger society.

Women's Skills

Table 7: Women's Skills–Statements and Results

Statements	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Mean

Women's technical skills are sufficient for cybersecurity in the banking sector.	2%	14%	22%	32%	30%	3.740
Women can use problem-solving skills in facing problems that might occur.	2%	8%	20%	26%	44%	4.020
The communication skills of women in cybersecurity are adequate.	0%	8%	20%	34%	38%	4.020
Women with people skills like establishing client confidence, being a team player, and encouraging loyalty are necessary to succeed in this field.	0%	0%	20%	36%	44%	4.240

Table 7 demonstrates attitudes about women's skills. Some critical skills are required for women entering this field. Based on the response, 32% agreed and 30% strongly agreed that women in Bahrain have sufficient technical skills to succeed in cybersecurity. However, 14% disagree and 2% strongly disagree, which suggests that they believe that women's technical skills are insufficient to succeed in the field. Problem-solving is an essential skill for information security as the systems face a lot of unforeseen problems. 44% of the respondents strongly agreed and 26% agreed that women could use problem-solving efficiently. 38% strongly agreed and 34% agreed that women have adequate communication skills for success in the field. In regard to their people skills, the respondents have a remarkable amount of confidence in Bahraini women, with a total of 80% agreeing (44% strongly agree, 36% agree) that they have the required people skills that will ensure success in this field with a mean of 4.240.

H_7: The greater the technical, communication, and people skills of women, the more success they can achieve in the field of the cybersecurity digitalized banking sector.

Cybersecurity Qualifications of Women in Banking

Table 8: Cybersecurity Qualifications of Women in Banking–Statements and Results

Statements	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree	Mean
Women working in the banks are aware of the Information Systems Audit and Control Association (ISACA) or other bank qualifications.	0%	8%	40%	28%	24%	3.680
Women working in banks have CSX Certification or Certified Information Security Manager (CISM) qualification.	4%	10%	46%	22%	18%	3.400

Table 8 shows statements and results concerning women in banks' cybersecurity qualifications. ISACA or any other qualifications are essential to achieve a high level of applying suitable standards in performing the tasks required and thus they enhance employee performance. Respondents believed that Bahraini women in banking are aware of this type of qualification based on the 28% who agreed and 24% who strongly agreed, while 8% specified that women were not aware of such qualifications. The majority of 46% chose neutral about Bahraini women in banks that are certified with CSX or CISM qualifications, which implies that they believe women and men are equally certified. However, 4% strongly disagreed, and 10% disagreed that women are certified. Such qualifications must be addressed in order to improve the quality of work and to raise awareness of the importance of such qualifications.

H_8: Women are increasing their cybersecurity qualifications in the cybersecurity digitalized banking sector.

Reliability Test

Cronbach Alpha is considered one of the most critical statistics tests in such studies since alpha is usually reported to develop scales used for affective constructs and attitudes. The score on Cronbach's Alpha reliability test was 0.844, for the eight factors that were examined related to women in cybersecurity through the digitalized banking sector. This indicates that the results are in the acceptable range and are reliable (Taber, 2018).

Analysis of Interviews

The Population

The interviews were conducted virtually with five decision-makers in the field of cybersecurity in the banking sector with varying years of experience, some with over 30 years of experience. One woman and four men were interviewed. The interview questions cover the same eight factors that affect women in cybersecurity through the digitalized banking sector examined in the questionnaire.

Results of Interviews

The interviews revolve around the eight factors that affect women in cybersecurity through the digitalized banking sector. The questions were asked, and the interviewers were given a space

to express their opinions related to the factors based on their experience. The following are the main results of the interviews:

- Women's challenges and limitations in entering the cybersecurity fields are that males have dominated the industry and women lack technical skills.
- Women's contributions in this field are equal to men's contributions. Their contributions will be to safeguard and manage cybersecurity threats to the business, core banking systems, and digital and internal systems.
- Women in the Fintech and Fintech ecosystem will develop the system and manage the risk of introducing Fintech's to the environment since they will be aware of the latest cybersecurity-related trends and regulations.
- Women will be involved from the start until the end of the digital transformation journey by ensuring that cybersecurity is an integral part and that all the risks are being managed at an acceptable level. They will ensure that all processes are done digitally.
- Women will contribute to the cybersecurity management strategy through in-depth knowledge of information technology in combination with cybersecurity and the enhancement of monitoring tools, and by raising awareness among organizations about the importance of cybersecurity. Women are working in focus teams to ensure that the international security standards are followed, and they are participating in upcoming research that involves new concepts and technologies.
- Women joining this field will have an economic and social impact as the awareness of the importance of cybersecurity to both business and personal life will increase. Others will be willing to enter the field to create a cyber-safe environment and trusted businesses, thus positively impacting the economy.
- Women must have some essential skills and in-depth knowledge of information technology related to cybersecurity. They should try to learn about risk management and information security policies and procedures. Also, some required skills for women in this field are the ability to learn fast, to read effectively, and to make good decisions.
- Women are aware of ISACA qualifications, but unfortunately the number of women certified in this field is minimal.

Women should understand the financial and internal systems and how technology evolves around them since they should be aware of the latest trends and regulations. They should get more involved in cybersecurity sessions, conferences, and studies. Furthermore, they have to be updated with cybersecurity news and measures required for safeguarding the banks' financial system. Women need to continue working towards the advancement and certification of their skills in this field. This will help women to compete in the cybersecurity banking field.

It has been noted that there are some points of view that differ between the survey group and the interview subjects. Regarding women's skills, the survey results clearly illustrated that women have technical and problem-solving skills, while the opinions of the interview subjects seem to be that women lack such skills. Furthermore, regarding women's qualifications and certifications in the field of cybersecurity, the survey results show that women are certified and aware of the need for required qualifications, but the interview subjects disagreed with this opinion and believe women need to be more qualified and certified in the cybersecurity field. Since the interview subjects were largely men (4 out of 5) compared to the survey respondents (52%

women), this gender difference in the qualitative versus quantitative parts of the study may have affected the results.

Conclusions

According to the research results, we could conclude that women will still face challenges and limitations within their careers in the cybersecurity banking sector. However, through hard work and empowerment in this field, they will undoubtedly contribute and have a significant role. The development of Fintech and digitalization depends upon women seeking to improve their knowledge of financial technologies and their performance in the banking sector. The cybersecurity management strategy will be built by the innovative ideas that women will contribute to this field. Economic growth and positive social impacts will be achieved by women's hard work and dedication to the cybersecurity of the financial sector. Women's skills and qualifications must keep on increasing to accommodate the fast development in this field.

Women should be able to work in cybersecurity in the banking sector in the same capacity as men since they have the necessary capabilities, motivation, and skills to succeed in this field. They are the future of cybersecurity in the Kingdom of Bahrain.

Notably, the community believes that women's power and intelligence could provide insight to improve the field, although women must still tackle the challenges and limitations that they face. They have to balance their family responsibilities and work. Women's contributions will undoubtedly lead to being promoted to higher cybersecurity positions in the banking sector. The technology revolution in the Kingdom of Bahrain is certainly growing fast through financial technology and the development of the digitalized banking field. Women will adopt these tasks and help improve them and might even introduce new ideas as they could have different perspectives in their creativity. Their cultural sense of obligation in regard to rules and regulations is high even though they need to be updated with knowledge of the cybersecurity world. The country's economy would benefit through their contributions in this field as qualifications are always essential, so women should embrace the certification process in this field.

Recommendations

The improvement role is a continuous process, so recommendations shall be provided to ensure women progress and advance in the cybersecurity field within the digitalized banking sector in the future. Some of the recommendations are as follows:

- Society's mentality must support the women in this field to manage a balance between their social life and work.
- It's important to raise awareness that the cybersecurity field is not limited to men since women have sufficient technical knowledge and could improve more through dedication and hard work.
- The government and banks can positively impact women's progress in this field, eventually leading to the economy's growth.
- The banks should offer training and development sessions for women employees in cybersecurity, because knowledge is the key to success.
- The banks must encourage women to be certified in this field as qualifications will support their working experience and promote innovation.
- Furthermore, women's awareness of the cybersecurity field should be increased through training sessions and opportunities to achieve professional qualifications.

Future Scope

Some issues that may be examined in the future are as follows:

- Further studies should be conducted related to this field due to the COVID-19 crisis and the stress of virtual work because of the unprecedented circumstance.
- Future studies could look into other countries' best practices and formulate policies based on the findings.
- More external and internal factors that affect women in this field should be investigated.
- The government should adopt and support future studies about women in this field and work on the improvement process based on statistics that might be found.

References

Al-Alawi, A. I. (2016). Status of Bahraini women in the banking and financial sector: challenges and opportunities. *Journal of International Women's Studies*, 17(4), 210-228. https://vc.bridgew.edu/jiws/vol17/iss4/15/

Al-Alawi, A. I., Elias, H., Zaid, F. A., Alroaili, M. S., & Al-Bassam, S. A. (2019). Factors Affecting Bahraini Women Working in the Engineering Fields. *Journal of International Women's Studies*, 20(7), 289-318. https://vc.bridgew.edu/jiws/vol20/iss7/19/

Al-Alawi, A. I., Al-Saffar, E., Almohammedsaleh, Z., Alotaibi, H., & Al-Alawi, E. I. (2021). A study of the effects of work-family conflict, family-work conflict, and work-life balance on Saudi female teachers' performance in the public education sector with job satisfaction as a moderator. *Journal of International Women's Studies*, 22(1), 486-503. https://vc.bridgew.edu/jiws/vol22/iss1/39/

Al-Alawi, A. I., & El Naggar, N. F. (2018). Factors affecting women leadership to reach top management and its impact on the economy: the case of the Kingdom of Bahrain. In *Arab Women and Their Evolving Roles in the Global Business Landscape* (pp. 87-119). IGI Global.

Al-Alawi, A. I., & Al-Bassam, S. A. (2021) Assessing The Factors of Cybersecurity Awareness in the Banking Sector, *Arab Gulf Journal of Scientific Research*, 37 (4) 2019: 17-32

Callen-Naviglia, J., & James, J. (2018). Fintech, Regtech and the Importance of Cybersecurity. *Issues in Information Systems*, *19*(3), 220-225. https://iacis.org/iis/2018/3_iis_2018_220-225.pdf

Chelly, M. L. (2016), Employees' Impact on Cyber Security. *Europe*, *614*, 73-90. https://res.cloudinary.com/peerlyst/image/upload/v1504865527/post-attachments/Employees_Impact_on_Cyber_Security_Oct_2016_fx29yd.pdf

Deen, L. (2019). Women in FINTECH. Women of Color Magazine, 19(1), 20-23. www.jstor.org/stable/26652803

DiCaprio, A., Yao, Y., & Simms, R. (2017). Women and Trade: Gender's impact on trade finance and Fintech. https://digitalcommons.ilr.cornell.edu/intl/680/

Fernandes, ARGC (2018). *Cybersecurity: Perspectives from Banking & Capital Markets, Insurance and Wealth & Asset Management sectors*. [Masters Dissertation, Nova School of Business and Economics], Carcavelos, Portugal. https://run.unl.pt/bitstream/10362/36548/1/Fernandes.A_2018.pdf

Giri, S. (2019). Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal. *Pramana Research Journal*, *9*(3), 662-672. https://www.pramanaresearch.org/gallery/prj-p576.pdf

James, J. E., & Callen, J. (2018). CYBERSECURITY CERTIFICATIONS MATTER. *Issues in Information Systems*, *19*(3). 193-201, https://iacis.org/iis/2018/3_iis_2018_193-201.pdf

Kembley Kay Lingelbach. (2018). *Perceptions of Female Cybersecurity Professionals Toward Factors that Encourage Females to the Cybersecurity Field.* Doctoral dissertation. Nova Southeastern University, NSUWorks, College of Engineering and Computing. (1056). https://nsuworks.nova.edu/gscis_etd/1056

Malmström, M., & Wincent, J. (2018). The Digitization of Banks Disproportionately Hurts Women Entrepreneurs. *Harvard Business Review*. https://www.diva-portal.org/smash/get/diva2:1255743/FULLTEXT01.pdf

Poster, W. R. (2018). Cybersecurity needs women, DOI:10.1038/d41586-018-03327-w

S. Bagchi-Sen, H. R. Rao, S. J. Upadhyaya and S. Chai. (2010). "Women in Cybersecurity: A Study of Career Advancement," *in IT Professional*, 12(1), 24-31, DOI: 10.1109/MITP.2010.39.

Shumba, R., Ferguson-Boucher, K., Sweeney, E., Taylor, C., Franklin, G., Turner, C., ... & Hall, L. (2013, June). Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation. In *Proceedings of the ITiCSE working group reports conference on innovation and technology in computer science education-working group reports* (pp. 1-14).https://doi.org/10.1145/2543882.2543883

Taber, K. S. (2018). The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education*, *48*(6), 1273-1296. DOI 10.1007/s11165-016-9602-2

Rowland, P., Podhradsky, A., & Plucker, S. (2018). Cyber: A Method for Empowering, Motivating, Educating and Anchoring Girls to a Cybersecurity Career Path. *In Proceedings of the 51st Hawaii International Conference on System Sciences*.DOI:10.24251/HICSS.2018.470.

Ugwuja, V. C., Ekunwe, P. A., & Henri-Ukoha, A. (2019). Cyber risks in electronic banking: exposures and cybersecurity preparedness of women agro-entrepreneurs in South-South Region of Nigeria. https://econpapers.repec.org/paper/agsaaae19/295693.htm

Zahout, M. (2017). Women in Cybersecurity. *McCloy Fellowship on Global Trends*, July 21, 2017. https://www.acgusa.org/wp-content/uploads/2017/08/McCloyFellowhip_Report-Zahout.pdf