

University of Bahrain

College Business Administration

Department Management & Marketing



A Study of Cybersecurity Behavior of Bahraini Employees in the Banking Sector

Thesis submitted in partial fulfillment of the requirements for the degree of (M.A)
in (Business Administration)

Prepared By
Zainab Jaafar Abdulla
20190218

Supervised by Dr.
Mourad Messaadia
Associate Professor

University of Bahrain,
June, 2024

Thesis Discussion, Committee Decision

University of Bahrain
Deanship of Graduate Studies
And scientific Research



جامعة البحرين
عمادة الدراسات العليا والبحث العلمي

Thesis Discussion Committee Decision

Student Name: Zainab Jaafar Abdulla Butraif	Student ID: 20190218
Department: Management & Marketing	College: Business administration
Program: Masters in Business Administration	
Thesis Title: A Study of Cybersecurity Behavior of Bahraini Employees in the Banking Sector	
Supervisor Name: Dr. Mourad Messaadia	Student GPA: 3.41

The Discussion Committee met on 27-Jun-24 In University of Bahrain. Upon discussing the student whose details are stated above in public, the discussion committee recommends the following:

PASS

The student is awarded a grade in the thesis subject.

- ☐ Without making any changes to the thesis.
- ☒ After making the modifications attached with this decision.

Discussion Committee Members Approval:

Name

1. Dr. Mourad Messaadia
2. Dr. Elsayed A.H. Elamir
3. Dr. Mohamed A. Benatia

(Advisor)

(Internal Examiner)

(External Examiner)

Signature

Click here to enter text.

Click here to enter text.

Click here to enter text.

6 | Approved at the University Council 6th meeting, 2013
In accordance with Decision No. 736/2013 dated 14/3/2013
Modified by University Council Decision No. 2043/2013 dated 20/11/2013.

Thesis Mark Distribution

Thesis Mark Distribution

The intellectual content of this thesis is the product of work and that all the assistance received in preparing this thesis and sources have been acknowledged. This work is an original in content.

Student Name: Zainab Jaafar Abdulla Butraif	ST ID: 20190218
Thesis Title: A Study of Cybersecurity Behavior of Bahraini Employees in the Banking Sector	

The total mark of the THESIS will be distributed as follows

Item	Mark
Thesis Report	64
Thesis Viva	26
Total	90

PART ONE: Thesis Report;

Students will be assessed for their thesis report on the basis of the following items:

Item	Mark
a.Abstract	4
Demonstration of a concise summary conveying the key items of the thesis.	
b.Introduction	9
Demonstration of a good explanation for the problem being considered in the thesis.	
c.Literature Review	10
Demonstration of an appropriate review for the relevant literature with the recent trends.	
d.Methods and Procedures	13
Demonstration of a good description for the data used. demonstration of understanding for the methods and procedures implemented.	
e.Results, Discussion, Conclusions and Recommendations	14
Demonstration of an appropriate of the thesis results. Demonstration of the reasonable discussion for the results and their implications. Demonstration of summarizing thesis findings and extracting possible recommendations.	
f. References	
Demonstration of a complete and unified- style for citation and referencing.	5
g.Format and Specifications	5
Demonstration of a well- structured report by adopting the university pre-determined format and specifications for thesis writing.	
h.Clarity and Grammar	4
Demonstration of clarity in writing with a correct grammar.	
Total	64

PART TWO: Thesis Viva;

Students will be assessed for their thesis viva on the basis of the following items:

Item	Mark
i. Background	4
Demonstration of having a good background about the thesis.	
j. Methodology	4
demonstration of understanding for the details and reasoning of the implemented methodology.	
k. Results Summary	5
Summarization of the results appropriately.	
l. Results Implications	4
Interoperation for the implications of the results.	
m. Potential Improvements	5
Demonstration of awareness about potential improvements of the results.	
n. Examination Panel Questions	4
Ability to answer the questions raised by the examination panel.	
Total	26

Examination Panel	Name	Signature	Date
Advisor	Dr. Mourad Messaadia	<i>Mourad Messaadia</i>	29/09/2024
Internal Examiner	Dr. Elsayed A.H. Elamir	<i>Elsayed A.H. Elamir</i>	
External Examiner	Dr. Mohamed A. Benatia	<i>Mohamed A. Benatia</i>	27/09/2024

Thesis Assessment Criteria

Above 80%	- Pass without corrections. - Pass with minor corrections. - Pass with major corrections, requires resubmission but no further oral examination. - Pass with major corrections, requires resubmission and a second oral examination. - Pass subject to doing further research, resubmission and a further oral examination.
Below 80%	Fail

Dedication

This thesis is dedicated to Bahrain, Arab countries, and other individuals from around the globe who are interested in this subject.

For the purpose of knowledge.

This research may shine a light on its topic for future generations.

Abstract in English

Purpose: The focus of this thesis is on studying the effect of cybersecurity culture on employees' behavior, specifically in the banking sector in Bahrain. The thesis will also evaluate the impact of external influences and internal mechanisms on security culture. This study will determine the impact of these factors on employee security behavior by identifying the most influential and the least influential of these factors. Furthermore, the purpose of this study is to identify the challenges faced by Bahraini organizations when achieving a high level of cybersecurity culture to enhance employee security behavior. The purpose of this research is to provide organizations with suggestions about how to achieve a high level of cybersecurity culture.

Design/ Methodology/ Approach: The research used a qualitative approach to acquire extensive knowledge of previous literature and to identify what previous literature suggested in relation to the research question. In order to create a conceptual framework for this research, the researcher used a qualitative approach, which was adapted to better suit the analysis of the thesis by the researcher. Comparatively, a quantitative approach was employed to obtain answers to Bahrain's research questions by using structured close-ended questions in focused group interviews. This study utilized the deductive methodology, which was selected so that the researcher could reason from generic to unique by using it. A prior research paper was used to develop the interview questions, which were modified to provide comprehensive primary data. Consequently, the interview questions were entered into an online data input system and coded, and the answers were designed using a LikertScale (a five-point rating scale). This study involved 108 Bahraini citizens, who were working in Bahrain at the time of the research. The participants were from different organizational sizes and different occupational levels within the banking sector. Additionally, random sampling was used to select respondents, and data was analyzed using the SVM through the machine learning pipeline.

Findings: The findings indicate that all proposed factors have an effect on cybersecurity culture in the banking sector in Bahrain, with the Organization Mechanisms factor having the greatest

influence whereas the External Influences factor has the least influence Employees' intentions to behave or their behavior on cybersecurity matters can be influenced by cybersecurity culture.

Keywords: Cybersecurity, cybersecurity culture, organizational culture, security awareness, employee behavior, Bahraini banking, Machine Learning, Support Vector Machine (SVM).

Dedication

In spite of the stress, the time management, the fake-diverting knowledge that organizations use for profits, the efforts to find truth, the waste of time, the joy of finding the truth, the paper, and the contribution it will make to the millions of available researches online, I dedicate this paper to:

His Majesty the King of Bahrain, Hamad bin Isa Al Khalifa

"No matter what nationality a person comes from; Bahrain is open to welcome them all. I have been committed to open up Bahrain to embrace people indiscriminately since I was a child. ", says His Majesty I quote, and this research clearly proves that Bahrain is open to people from all nations to come, work and live here.

We appreciate your continued leadership and wisdom.

H.E. President of University of Bahrain, Dr. Fuad Mohammed Al-Ansari his career in education reform is unquestionable, and Bahrain is proud to have someone such as him as a leader. He is the President of the University of Bahrain, Bahrain's most valuable higher education institution that incubates over 30,000 students.

Head of Management and Marketing Department, Dr. Waleed A. Aziz in response to my endless emails, phone calls, and questions regarding administration, thesis requirements, processes, and procedures, I greatly appreciate your undivided attention.

Dean of College of Business Administration, Dr. Abdulla Al Jalahma Thank you for your invaluable support, guidance, and advice throughout my Masters' studies at the University of Bahrain.

Professor of Management & Information Systems, Dr. Adel Al-Alawi, I am thankful to my wonderful mentor, for his patience, tolerance, great spirit, and contribution of knowledge, wisdom, and encouragement throughout my MBA education.

Associate Professor, Dr. Mourad Messaddia, I greatly appreciated your critical inputs during the completion of my thesis and your high standards of research led to the continuous involvement of my cerebral hemispheres in a continuous in-depth analysis.

Acknowledgement

The first thing I want to do is acknowledge the existence of Allah Almighty as the only true God, and I would like to take this opportunity to thank Him above all else, because He is the worthiest of all praise and worship, and I am simply a humble servant who has the desire to learn, knowledge that He created and made available to us. I praise Him for life, strength, knowledge, setting of the environment, people, and all things that contributed to realizing this success.

Second, although some may believe I was lucky, I believe I am blessed to have met Dr. Adel Al-Alawi, Professor of Management & Information Systems at University of Bahrain, during the heart of the pandemic, who was my instructor, mentor, inspiration, and a golden human being. In addition to providing me with insight into best practices, tools, and free beneficial knowledge throughout my years of study, he introduced me to my great advisor and supervisor, Dr. Mourad Messadia, without whom I would not have been able to complete this thesis.

Thirdly, I would like to thank my dear advisor and supervisor, Dr. Mourad Messadia, for being my guardian advisor. You met with me often, responded to so many emails, shared insights into other projects with me and helped me get through the worrying qualitative and quantitative analysis requirements for my thesis.

In the end, I want to thank some people without naming them, who they know I mean them, who were the light and the hope in my studies from the beginning, and my family for their support, without which I wouldn't have been where I am today. Please accept my sincerest gratitude from the bottom of my heart.

I am grateful to all of you. Be Blessed.

Last but not least, this goes to Bahrain and the world, for Arab-based researchers to become one day leaders of global scientific research.

Thank you,

Zainab Butraif

Table of Contents

Thesis Discussion, Committee Decision	B
Thesis Mark Distribution.....	C
Dedication.....	E
Abstract in English	F
Dedication.....	H
Acknowledgement.....	I
Table of Contents.....	J
List of Tables	N
List of Figures.....	P
Table of Abbreviations.....	S
1.1. Introduction.....	1
1.2. Research Problem	2
1.3. Research Questions	4
1.4. Research Objectives.....	5
1.5. Research Significance	5
1.6. The Study Setting.....	7
2.3. The Human Factor and Data Breach.....	20
2.4.1. Definitions and terms.....	22
2.4.2. Cybersecurity Objectives.....	23
2.4.3. Cybersecurity Culture.....	24
2.4.3.1 Organizational Cybersecurity Culture	25
2.4.4. Cybersecurity External Influences.....	26
2.4.4.1 Societal Cybersecurity Culture.....	26
2.4.4.2. External Rules and Regulations.....	27
2.4.4.3. Peer Institutions	28
2.4.5. Cybersecurity Internal Mechanisms	29
2.4.5.1. Cybersecurity Culture Leadership	29
2.4.5.2. Performance Evaluations.....	32
2.4.5.3. Rewards and Punishments	33
2.4.5.4. Organizational Learning	34
2.4.5.5. Cybersecurity Training	35
2.4.5.6. Communications Channel.....	36
2.4.5.7. Cybersecurity Budget	36
2.4.6. Beliefs, Values & Attitudes	37
2.4.6. Cybersecurity Employee Behavior	38
2.4.7. Technology Acceptance Theories	39
2.5. Theory of Acceptance and Use of Technology (UTAUT2)	44
2.6. Limitation of UATUT 2	46
2.7. Machine Learning in Technology Acceptance	47

2.8. Cybersecurity working group in the GCC	49
2.9. Status of Bahraini Cybercrimes	51
2.10. An Overview of Banking Sector Importance	53
2.11. Research Gap	54
2.12. Chapter Summary	56
Chapter Three: Theoretical Framework, Methods, and Procedures	58
3.1. Introduction	58
3.2. Theoretical Framework	60
3.2.1. Previous Studies	60
3.2.2. Research Variables	68
3.2.3. Conceptual Framework	70
3.2.4. Research Hypothesis	71
3.3. Research Philosophy	72
3.4. Research Design	73
3.5. Research Approach	79
3.6. Operational & Conceptual Definitions of Variables	81
3.7. Research Strategy	83
3.8. Data Collection Method	84
3.9. Sample Selection Method	87
3.10. Research Flowchart	91
91	
3.11. Research Sample and Interpretation of Interview Questions	92
3.12. Interview Questions Development	97
3.13. Machine Learning Pipeline	102
3.13.1. Machine Learning	102
3.13.1.1. Introduction	102
3.13.1.2. Machine Learning Steps	102
3.13.1.3. Machine Learning Techniques	105
3.13.1.4. Learning Techniques Illustration	106
3.13.1.5. Supervised Learning	107
3.13.2. Support Vector Machines SVM	107
3.13.7. Python	109
3.13.8. Example of Machine Learning in Practice	110
3.13.9. The Deployment & Selection of the Analysis Methodology	112
3.14. Ethical Considerations	114
3.15. Chapter Summary	115
Chapter Four: Data Analysis, Results, and Discussions	118
4.1. Introduction	118
4.2. Interview Findings	119
4.2.1. Data Editing and Coding	120
4.2.2. Data Entry	121

4.2.3. Interviews Pre-Testing.....	121
4.2.4. Reliability analysis (Pilot Testing)	123
4.2.5. Preparing and Cleaning the Data	123
4.2.6. General Question	123
4.2.7. Interviewee Profile	124
4.2.7.2. Age.....	125
4.2.7.3. Marital Status.....	126
4.2.7.4. Education Level: University Degree	127
4.2.7.9. Summary of Participants Profile.....	127
4.2.8. Independent and Dependent Variable Questions	128
4.2.8.1. Independent Variable Questions	129
4.2.8.2. Moderating Variable Questions	132
4.2.8.3. Dependent Variable Questions.....	135
4.2.8.4. Summary of All Variable Questions	138
4.2.8.5. Interview Results of Variable Questions.....	146
4.2.8.5. Interview Results of Variable Questions.....	151
4.2.8.6. Interview Results of Dependent Variable Questions	158
4.3. Analysis: The Machine Learning Pipeline	163
4.3.1. Dataset Collection	163
4.3.2. Data Preparation	164
4.3.3. Feature Engineering.....	167
4.3.3.1. Correlation	167
4.3.3.2. Mean and Standard Deviation	169
4.3.4. Selection of Model	171
4.3.5. Training the Model	173
4.3.6. Model Evaluation	176
4.3.7. Result and Discussion.....	180
4.3.7.1. Parameters Importance	180
4.3.7.2. External Influences	190
4.3.7.3. Organizational Mechanisms	191
4.3.7.4. Overall Factors Importance Measure	193
4.3.7.5. Cybersecurity Culture.....	194
4.3.7.6. Behavior Intention	196
4.3.7.6. Cybersecurity Behavior	198
4.3.8. Research Hypothesis Testing.....	198
4.3.9. Preview of Research Study Results	199
4. 4. Chapter Summary	201
Chapter Five: Conclusion and Recommendations	205
5.1. Introduction.....	205
2. The Theoretical and Practical Implications	205
5.2. The Theoretical and Practical Implications.....	206

5.2.1. Theoretical Implications	206
5.2.2. Practical Implications	207
5.3. Research Limitations	209
5.4. Suggestions for Future Researchers	210
5.5. Recommendations	211
5.6. Conclusion	213
References	217
Appendices.....	237

List of Tables

Table 1: A comparison of high and low performance cultures adapted from Warrick (2017)	52
Table 2: Researches on Cybersecurity Measurement Models	90
Table 3: Research Variables of the Study	91
Table 4: Sub factors of Independent Variables of the Study	92
Table 5: Quantitative Research Design Strategies	99
Table 6: Qualitative Research Design Strategies	100
Table 7: Types of Definitions of Variables	105
Table 8: Summary of the operational and conceptual definitions of the variables	106
Table 9: Methods of collecting data	108
Table 10: Sample selection methods for a population	112
Table 11: Response Rate of Interviews in This Study	117
Table 12: Type of Interview Conducted in This Study (Online, In-Person)	118
Table 13: 5-point Likert Scale System	118
Table 14: Interview sections and descriptions	121
Table 15: Case Study Examples of Cybersecurity Culture Elements (Huang & Pearlson, 2019)	122
Table 16: Factors and Sub factors of the Interview Questions of this Study	125
Table 17: The steps of machine learning	129
Table 18: Description of Machine Learning Technique	130
Table 19: Practical Applications of Machine Learning	136
Table 20: Coding explanations for Interview Questions	141
Table 21: Likert scale with 5 points	141
Table 22: Results of the interview - Gender	148
Table 23: Results of the interview – Age	149
Table 24: Results of the interview – Marital Status	150
Table 25: Interview Result – Education Level	151
Table 26: Interview Result – Summary of Respondents Profile	153
Table 27: Independent Variable Questions – External Influences.....	155

Table 28: Independent Variable Questions – Organizational Mechanisms	157
Table 29: Summary of All Variable Questions	159
Table 30: Study Parameters Correlated	182
Table 31: Parameter Means and Standard Deviations	184
Table 32: Variable Means and Standard Deviations	185
Table 33: Detailed Feature Ranking	202
Table 34: Ranking Scores based on external influences	205
Table 35: Ranking Scores based on Organizational Mechanisms	206
Table 36: Factors Importance Measure and Ranking	208
Table 37: Ranking Scores based on Cybersecurity Culture	210
Table 38: Ranking Scores based on Behavior Intention	212
Table 39: Research Hypothesis Testing	214

List of Figures

Figure 1: Thesis Structure.....	32
Figure 2: Huang and Pearlson (2019) Organizational Mechanisms for Cybersecurity.....	49
Figure 3: Adapted from Huang & Pearlson (2019) the three organizational levels of cybersecurity culture	57
Figure 4: A Chronology of Acceptance Models Development	63
Figure 5: Conceptual Framework of the UTAUT2	66
Figure 6: Research Gap	77
Figure 7: Study Conceptual Framework	92
Figure 8: Research Approaches Methods	102
Figure 9: Research Flowchart of the Study.....	114
Figure 10: Machine Learning Steps	126
Figure 11: Illustration of Machine Learning Techniques	130
Figure 12: Interview Result – Gender	148
Figure 13: Interview Result – Age	149
Figure 14: Interview Result – Marital Status	150
Figure 15: Interview Result – Education Level	151
Figure 16: Interview Result – EI1	160
Figure 17: Interview Result – EI2	160
Figure 18: Interview Result – EI3	161
Figure 19: Interview Result – OM1	161
Figure 20: Interview Result – OM2	162
Figure 21: Interview Result – OM4	163
Figure 22: Interview Result – OM5	163
Figure 23: Interview Result – OM7	164
Figure 24: Interview Result – CSC1	164
Figure 25: Interview Result – CSC2	165
Figure 26: Interview Result – CSC3	165
Figure 27: Interview Result – CSC4	166
Figure 28: Interview Result – CSC5	166

Figure 29: Interview Result – CSC6	167
Figure 30: Interview Result – CSC7	167
Figure 31: Interview Result – CSC8	168
Figure 32: Interview Result – CSC9	168
Figure 33: Interview Result – CSC10	169
Figure 34: Interview Result – CSC11	169
Figure 35: Interview Result – CSC12	170
Figure 36: Interview Result – CSC13	170
Figure 37: Interview Result – CSC14	171
Figure 38: Interview Result – BI2	171
Figure 39: Interview Result – BI3	172
Figure 40: Interview Result – BI4	172
Figure 41: Interview Result – CSB1	173
Figure 42: Interview Result – CSB2	173
Figure 43: Interview Result – CSB3	174
Figure 44: Interview Result – CSB4	174
Figure 45: Interview Result – CSB5	175
Figure 46: Interviews Data in Excel Sheet Program	175
Figure 47: Interviews Data Input in the Machine Learning Pipeline	177
Figure 48: Values of External Influences and Organizational Mechanisms in Python	178
Figure 49: Pre-removal Correlation Graph	179
Figure 50: Variables with high correlation	180
Figure 51: Parameter Means and Standard Deviation	181
Figure 52: Data Subset Training and Testing Machine Learning Code	184
Figure 53: The import of datasets in machine learning	187
Figure 54: Python code for splitting a dataset into Train and Test Sets	188
Figure 55: SVM classifier model initialization	188
Figure 56: Model fitting with SVM	188
Figure 57: Making predictions	189
Figure 58: Performance evaluation of the model	189
Figure 59: An example of a confusion matrix	190

Figure 60: The entries of the confusion matrix	191
Figure 61: Study Confusion Matrix	192
Figure 62: SVM Code of Parameter Importance	194
Figure 63: Scores computed by SVM	194
Figure 64: Features scored in detail	190
Figure 65: Rankings by feature detail	202
Figure 66: An extract of the Python feature ranking graph	202
Figure 67: Ranking Scores based on external influences	204
Figure 68: Ranking Scores based on Organizational Mechanisms	206
Figure 69: Factors Importance Measure and Ranking	207

Table of Abbreviations

Abbreviation	Full Form
BI	Behavior Intention
CSB	Cybersecurity Behavior
CSC	Cybersecurity Culture
EI	External Influences
OM	Organizational Mechanisms
SVM	Support Vector Machine

Chapter One: Introduction to the Study

1.1. Introduction

With the internet, we can advertise our business across the globe at little to no cost and with minimal effort, within a short period of time, and with very little effort. Because the internet was never built to track user behavior. The Internet was designed for resource sharing between autonomous computers and as a community platform for researchers to collaborate. While the internet provides a great number of benefits, it also provides equal opportunity for cyberterrorists and hackers. A large amount of confidential information and data is collected, processed, and stored by governments, organizations, financial institutions, universities, and other businesses, and is transmitted over networks to other computers. Since more governments are converting to internet-based services to increase interactions, they are transforming their major services online. In today's environment of continuously growing cyber-attacks, it is imperative to secure sensitive business and personal information, as well as to protect national security.

With the advent of computer networks, cyber security systems have become increasingly important (Gumusbas et al., 2021). Government's increased online presence and social presence offer the potential to increase citizen engagement and citizen co-production, but they can also increase the risk of increased government endpoint security vulnerabilities. As the Internet and mobile connections become more diverse, there are more potential entry points for data breaches and malicious hacker attacks (Chatfield & Reddick, 2017). National and government priorities have been placed on cybersecurity. Today's communities rely on cyberspace to

provide essential and valuable services, as well as to face challenges and threats. Individuals are more likely to follow cybersecurity procedures when they observe that their peers routinely do so, because they are concerned about being left out if they act differently (Alshaikh, 2020). There are many breaches of security in organizations, and many of these breaches are linked to human error. In order to increase their level of security awareness and capability of engaging in safe cybersecurity behaviors, the organizations need to increase employee security awareness, and many psychological and social factors influence the employees' cybersecurity behaviors (Anwar et al., 2017).

Using selected Bahraini banks as case studies, this study explores the practices of implementing a cybersecurity culture within them. This research was conducted on selected banks primarily because of their importance to the banking sector and to see how they handle cybersecurity in their organization.

Following is the rest of the paper: first, a brief introduction to IT security culture is presented as a background section. In the second section, the methodology of the research is explained. In the third section, the results and analysis of the case study include key initiatives for building cybersecurity culture, followed by a framework for building cybersecurity culture and its effectiveness. Lastly, we discuss the theory and practice implications for the development of their cybersecurity culture, as well as directions for future work.

1.2. Research Problem

Cybersecurity is one of the major issues modern society faces. Further, it is a key element for an organization's relevant managers to limit the risk of cybercrime. Because of the widespread use of electronic services (e-services), cyberattacks continue to increase in frequency and sophistication, posing a threat to financial

operations. Security threats and risks that are not adequately addressed pose serious threats and challenges to the world's information societies (Kianpour et al., 2022). Although there is limited empirical research on cyber risk disclosure trends and practices among public companies, cybersecurity risks are significant and may have a material effect on business operations and public reporting (Gao et al., 2020). Researchers have focused on improving compliance behavior in the area of security in recent years (Donalds & Osei-Bryson, 2020). In 2013, 40 million credit and debit card numbers were compromised in a cyber-breach at Target stores in the U.S. (Beuran et al., 2017). It was reported in 2015 that the Japan Pension Service had been hacked, which exposed the personal information of 1.25 million of its users (Beuran et al., 2017). Over 500 million Yahoo accounts were compromised in 2014 by a breach that recently emerged. It has been called the largest breach in Internet history (Beuran et al., 2017). Consequently, cybersecurity education and training are becoming increasingly relevant, as they are the only means of preventing and handling such breaches (Beuran et al., 2017). Many training programs are available, most of them paid, but there are also some that are free. For example, CYDER (MIC, 2016) is a hands-on training program coordinated by the Ministry of Internal Affairs and Communications for IT personnel of government organizations and large companies in Japan (Beuran et al., 2017). Moreover, The WASForum's Hardening Project (WASForum, 2016) is a security contest in which teams of security specialists and IT professionals compete for a realistic company network to determine what kind of security improvements they can provide (Beuran et al., 2017). Additionally, in Japan, enPiT-Security (SecCap) (enPiT University Consortium, 2016) is an education program to be offered to students with support from the Ministry of Education, Culture, Sports, Science and Technology, and coordinated through a consortium of five universities (Beuran et

al., 2017). A growing number of cyberattacks causes a range of critical costs to people and organizations, making cybersecurity a critical component of enterprise risk management (Lee, 2021). It is estimated that there were 130 security breaches in 2017 and 145 in 2018, representing an increase of 11% in a year. This was accompanied by penalties, reputational harm, a decrease in stock value, compliance breaches, and privacy breaches (Lee, 2021).

To protect its confidential information from leaking, each corporation in the Kingdom adopts and develops a cybersecurity policy. Hence, Cybersecurity improvements enhance customer trust and increase revenue potential costs (Lee, 2021). Accordingly, the problem of this research lies in the lack of proper and effective awareness, education, and training of cybersecurity among employees who work for Bahraini government agencies.

1.3. Research Questions

For the research to accomplish its goals and objectives, several questions will need to be answered. In Cyberspace, cybersecurity refers to a system designed to safeguard a network and data of an organization against different types of attacks.

Research questions have been formulated as a first step; they guide the search, inclusion and exclusion criteria, and results assessment. In order to build the fundamentals and pathways for the study, the following questions have been posed:

RQ1: How is Bahrain's banking sector adopting cybersecurity culture through external influences and organizational mechanisms?

RQ2: How can machine learning methods contribute to Bahrain's banking sector adoption of cybersecurity culture?

RQ3: What effect does cybersecurity culture have on banking employees' behavior?

1.4. Research Objectives

In this study, we will investigate the relationship between cybersecurity awareness, education, and training among government employees. As well as achieving the following objectives, the research aims to:

1. Examine the effect of cybersecurity culture on bank employees' behavior.
2. Understand how banking institutions are implementing cybersecurity culture by using external influences and organizational mechanisms (Huang & Pearson, 2019).
3. Explore existing adoption models and tackle their limitations by using machine learning approaches and develop recommendations for banking policymakers, cybersecurity practitioners, and academics on how to create a strong cybersecurity culture and improve the security awareness and behaviors of bank employees.

1.5. Research Significance

According to newspaper reports, academic studies, security-related conference proceedings, and many other studies, cybersecurity is a topic that is currently capturing considerable interest and attention across a wide spectrum of stakeholders (von Solms & von Solms, 2018). As a topic, it grows in importance and significance from month to month, while its impact and consequences are ever-expanding. Furthermore, the study has several benefits from a variety of perspectives. Firstly, an effective cybersecurity framework plays a crucial role in spreading cybersecurity practices across a nation (Dedeke & Masterson, 2019).

Secondly, Given the huge impact recent high-profile cyber-attacks have had on companies' financial, reputational, and legal standing, the disclosure of cybersecurity risks faces by public companies and how these risks are managed is becoming increasingly important to investors, governments, consumers, vendors, and other stakeholders to make informed decisions (Gao et al., 2020). Thirdly, Cyber threats and attacks have increased in recent years, and this is one of reasons that led the Securities and Exchange Commission (SEC) to become more aggressive in its examination of public companies' disclosures of dangers and the cybersecurity policies, processes, and controls that they have in place to deal with them (Gao et al., 2020).

Based on how the research is conducted and the organization that will apply it, the outcome may be either positive or negative. As a result of the positive impact scenario, any organization seeking to improve employee security behavior and thus reducing security threats, may incorporate employee security behavior as a concept into their cybersecurity risk assessment, resulting in the loss of a huge amount of money in many cases, and by assessing the risk associated with various security controls, they could reduce their loss if and when those controls fail to protect their cyber systems and assets. A company that anticipates a negative impact on its financials (i.e., the cost of security training exceeds its benefits) would choose not to spend that money, thus saving (reducing) their expense. This study should be even more significant given that a positive or negative impact can help organizations save costs.

1.6. The Study Setting

The research is structured into five major chapters to achieve the research objectives:

Chapter 1: Introduction to the Study

An overview of the subject is presented in this chapter, which serves as a transition from the general framework to the paper's main topic. Among the topics covered in the introduction chapter are:

1. Introduction
2. Research Problem
3. Research Questions
4. Research Objectives
5. Research Significance
6. The Study Setting
7. Research Terminologies
8. Chapter Summary

Chapter 2: Literature Review

We begin this chapter by reviewing previous studies concerning cybercrime, cybersecurity, and the culture of cybersecurity. After adopting Huang and Pearlson (2019) research, we clarified the external influences and internal mechanisms that influence organizational cybersecurity culture. It was then explained in detail what cybersecurity culture is and how employees behave when it comes to security. Following that, the research focused on explaining what types of technology

acceptance models were used to achieve the research's goal. The last point discussed the level of cybersecurity in GCC and Kingdom of Bahrain, and the importance of the Governmental Sector, since the research will be focused mainly on this sector.

Research has been conducted on the following topics:

1. Introduction
2. The concept of Cybercrime
3. The Human Factor and Data Breach
4. Definitions and terms
5. Cybersecurity Objectives
6. Cybersecurity Culture
7. Organizational Cybersecurity
8. Cybersecurity External Influences
9. Cybersecurity Internal Mechanisms
10. Beliefs, Values & Attitudes
11. Cybersecurity Employee Behavior
12. Theory of Acceptance and Use of Technology (UTAUT2)
13. Limitation of UTAUT 2
14. Machine Learning in Technology Acceptance
15. Cybersecurity and cybersecurity working group in the GCC
16. Status of Bahraini Cybercrimes

17. An Overview of Government Sector Importance

18. Research Gap

19. Chapter Summary

Chapter 3: Theoretical Framework, Methods, and Procedures

This chapter presents a detailed theoretical analysis of the topic of the study that can be categorized into several categories. In this chapter, the research framework for conducting this research is described; it is followed by a research hypothesis derived from the framework and concludes with a summary. Furthermore, this chapter discusses the methodology used to analyze the research questions, the research design, the population and sample, interview questions, research tool, data collection / procedures, and statistical methods. We conclude this chapter with a summary.

This chapter includes the following topics:

1. Introduction
2. Theoretical Framework
 - o Previous Studies
 - o Research Variables
 - o Conceptual Framework
 - o Research Hypothesis
3. Research Philosophy
4. Research Design
5. Research Approach

6. Operational & Conceptual Definitions
7. Research Strategy
8. Data Collection Method
9. Sample Selection Method
10. Research Flowchart
11. Research Sample & Interpretation of Interview Questions
12. Interview Questions Development
13. Machine Learning Pipeline
 - o Machine Learning
 - o Support Vector Machines (SVM)
 - o Python
 - o Example of Machine Learning in Practice
 - o The Deployment & Selection of the Analysis Methodology
14. Ethical Considerations
15. Chapter Summary

Chapter 4: Data Analysis, Results, and Discussions

This chapter summarizes the analysis' findings, discusses them, and offers recommendations. Furthermore, it explains the study's findings in detail as well as analyzes the questionnaire results. It contains analysis of the data based on the machine learning pipeline and the use of SVM algorithm. During this chapter, the analysis of the data is also used to reject or accept hypotheses. This section provides

a brief overview of the entire analysis performed as well as a clarification of the study results.

Specifically, it comprises the following sections:

- Introduction 2. Interview Findings
 - o Data Editing and Coding
 - o Data Entry
 - o Interviews Pre-Testing
 - o Reliability analysis (Pilot Testing)
 - o Preparing and Cleaning the Data
 - o General Questions
 - o Interviewee Profile
 - o Independent and Dependent Variable Questions
- Analysis
 - o Dataset Collection
 - o Data Preparation
 - o Feature Engineering ▪ Correlation ▪ Mean and Standard Deviation
 - o Selection of Model
 - o Training the Model o Model Evaluation
 - o Results and Discussion
 - Parameters Importance

- External Influences
- Internal Mechanisms
- o Research Hypothesis Testing
- o Preview of Research Study Results
- o Chapter Summary

Chapter 5: Conclusion and Recommendations

In this chapter, we summarize the study and present the conclusions, and we discuss theoretical and practical implications, research limitations, and suggestions for future investigation.

Throughout this chapter, you will find the following sections:

1. Introduction
2. The Theoretical and Practical Implications
3. Research Limitations
4. Suggestions for Future Researchers
5. Recommendations
6. Conclusion

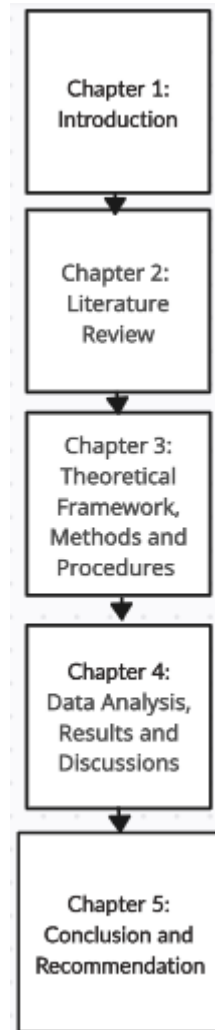


Figure 1: Thesis Structure

1.7. Research Terminologies

Going through the literature of cybersecurity, and revise the models proposed in prior studies, this study use the success factors by Huang & Pearson (2019) as appropriate and by using UTAUT 2 model to evaluate the case of government organization in Bahrain with the application of cybersecurity culture among the governmental employees. The variables used through the research are as the following:

Employee security behavior: independent variable; Human errors often play a role in security breaches within organizations. As a result, the organizations need to increase employee awareness of security and capability to engage in safe cybersecurity behaviors. Cybersecurity behaviors are influenced by a variety of psychological and social factors (Anwar et al., 2017). Alshaikh (2020) explained cybersecurity behavior: in order to simplify security policy and translate it into behavioral actions and goals, it is vital to identify key cybersecurity behaviors. Employees and cybersecurity teams alike need to improve their cybersecurity behavior. It will be clear to all employees what actions they need to take to comply with the security policy. Individuals are more likely to follow the same cybersecurity procedure when they observe that their peers are doing the same, worrying that they might be left out if they act differently (Li et al., 2019). Huang, K., & Pearlson, K. (2019), because cybersecurity is more than a technical issue, employers need to rely on their employees' behavior to prevent cyberattacks. Cyber-based vulnerability is ultimately determined by employee behavior.

Organizational mechanisms: dependent variable; Huang, K., & Pearlson, K. (2019) described it as the beliefs, values, and attitudes of an organization, which are a form of unwritten rules, and, therefore, culture, which are shaped by the actions of managers and leaders, including the mechanism of management.

External Influences: dependent variable, Huang, K., & Pearlson, K. (2019) characterized cybersecurity as attitudes, beliefs, and values that are influenced by other factors. By way of example, the more the media reports on cyber breaches, the more people become aware of cyber risks.

At the center of the model is cybersecurity culture; it is defined by three factors: values, beliefs, and attitudes. It is unwritten rules that everyone knows but that few

can articulate. Nevertheless, they are evident in the actions of leaders, groups, and individuals.

1.8. Chapter Summary

Every study has a story and objectives assembled behind it; thus, this chapter presented a holistic overview of why such a study was done. Detailed background information about the study's topic chosen and a close look on the cybersecurity behavior in the public frame in the Kingdom of Bahrain, were provided, along with the research problem declaration, additionally introduced sections which sat up the research questions and objectives, besides research significance and contributions, also main terminologies and finally the research structure and summary. The next chapter will move to deeper definitions and terms, theories and models that support the study of cybersecurity in Bahrain.

Chapter Two: Literature Review

2.1. Introduction

Even though cybercrime and victimization from cybercrime have gained considerable (academic) attention. There are still few studies that examine how cybersecurity affects top management, employees, and their behavior. Through previous studies and security implications, this chapter focuses on the CSA in the banking sector. Firstly, the author will introduce definitions and terms related to her study, followed by a summary of previous studies in the same area from different angles, and finally the main theories of the study will illustrate the framework and generate the hypothesis of the study.

Cybersecurity difficulties exist when computers, related technologies, and a networked system are utilized to damage the victim. Therefore, the definition of cybercrime is the use of technology to conduct crimes. The victim of violent cybercrime can suffer harm or injury. Injuries can be physical (such as lost data or revenue) or intangible (such as malfunctioning systems or a loss of reputation), depending on the nature. Organic victims (like a human) and non-organic victims (like robots or drones) are the two types of cybersecurity victims. (Chandra & Snowe, 2020)

Cybersecurity is a network system security protection for the organization's information against any cyber threats, which acts as a prevention against any damage to, or destruction of, vulnerable databases. Additionally, every business should protect its network against vulnerabilities caused by the network design, end user carelessness, inheritance of a weak technology, or misconfigured hardware and software (Spalević, 2014).

Hearth and Rao (2009) argue that cyber security cannot be achieved by technology alone. As the cybersecurity of an organization relies heavily on user behavior, regardless of how strong its technical defenses may be (Rhee et al., 2009). The Kaspersky (2018) report stated that 40% of workplaces hide incidents when they happen in 40% of industries worldwide. Additionally, 52% of industries admit workers are their biggest weakness when it comes to cybersecurity, with their irresponsible activities putting corporation cybersecurity strategies at risk. The findings of Kaspersky's survey showed that industries definitely intend to be concerned about cybersecurity risks for their personnel. As Gelles (2016) points out, employees may make errors that pose a threat to the data and systems of their organization through negligence, an accident, or a lack of the training necessary to teach them how to behave and act appropriately to support their organization.

The training of employees is essential to raise awareness and motivate them to take countermeasures even when cyber threats do not directly relate to their work. This is one of the best-known methods for protecting business against future cyber threats, with staff training and engagement key to creating awareness among workers and motivating them to address cyber threats (Bada et al., 2014).

It is also important to point out that cyber criminals have continued to develop and grow their techniques, along with threats to network security. These threats include external threats, internal threats, structured threats and unstructured threats. Threats can be divided into two types, unstructured and structured. Unstructured threats are created by people with little hacking experience and are executed in order to challenge their skills (Al-Alawi, 2014). In contrast, structured threats are hackers who are motivated, understand, and develop hacker techniques to penetrate a

business, and are specialized in cybercrime, such as fraud and information theft. It is also crucial to protect against external as well as internal threats in terms of data breaches, and the security strategies need to adequately address both (Aloul, 2012).

2.2. The concept of Cybercrime

The word cybercrime is an amalgamation of the word “cyber” and “crime”. It was Wiener (1948) who first used the word "cyber" in referring to machines and animals communicating with each other (Ho, Ko, & Mazerolle, 2022).

Exactly what is cybercrime? There are many researchers who agree that cybercrime involves any illicit activity carried out through a computer, but there is some disagreement as to where it takes place. According to Chung et al., (2006) cybercrime is an illegal activity carried out through computer-mediated systems. Cybercrime has a long-term negative impact on victims because it is hard to detect and difficult to prevent after it has occurred (Gunjan et al., 2013). The term cybercrime is defined by R Nagpal of the Asian School of Cyber Law as an illegal act in which a computer is either used as a tool or a target. In addition to desktop computers, sophisticated watches, mobile phones, PDAs (Personal Digital Assistants) and a host of these gadgets are used (Gunjan et al., 2013).

How does cybercrime differ from other types of crime? Like traditional crime, Cybercrime has many different facets and occurs in a wide variety of scenarios and environments. Current definitions of Cybercrime have evolved experientially. They differ depending on the perception of both observer/protector and victim, and are partly a function of computer-related crimes geographic evolution (Gordon & Ford, 2006). Cybercrime can include computer hacking, Internet fraud, virus spreading, and theft of confidential information (Chung et al., 2006).

Cybercrime differs from other types of crime in that hackers can hide behind computers rather than be confronted physically.

The concept of cybercrimes in society is also explained by the concept that whenever the rate of investment return is high and the risk is low, a large number of people will benefit from this situation, which means that accessing and attempting to use valuable information can produce a high return.

The motivations behind cybercrime are economic, personal, ideological, and structural. In cybercrime, the main goal is to obtain money or damage reputations by damaging IQ equipment or IT-based services of businesses or government. Some hackers may view this as an opportunity for personal gain and vendettas. A cybercriminal can also make money by selling stolen information on the Black Market (Smith, Jones, Johnson, & Smith, 2019).

Aside from that, cybercrime damages the economy, trade, and competitiveness. As businesses move their operations online and consumers connect to the internet, the cost of cybercrime will likely increase.

In the world of cybercrime, there are many types. In accordance with Smith, Jones, Johnson, & Smith, (2019), cybercrime is constantly evolving, so businesses must protect data and continually evaluate ways to prevent cyberattacks. Forgery, fraud, theft, mischief, defamation, and web defacement are all criminal activities that have evolved from computer abuse (Gunjan et al., 2013).

AAG IT support services for businesses highlighted the cost of cybercrime in their website, such as 39% of UK businesses reporting that they had been hit by a cyberattack in the past few years as of 2022, cybercrime has affected 53.35 million US citizens. Cyber threats have been greatly affected by Russia's invasion of Ukraine. Since the war began, Russian-based phishing attacks have increased

eightfold against US and European companies. It is estimated that 3.6 million Russian internet users experienced breaches in the first quarter of 2022, an increase of 11% month-over-month.

There is no way that most modern-day crimes could have been committed without the aid of computers, whether it is the famous attacks on the "World Trade Center" in the USA, serial blasts, the Taj hotel in India, or hacked web portals (Gunjan et al., 2013).

There is no doubt that cybercrime is the greatest threat to publicly traded companies today. An essential aspect of technology management is defending company information systems from cybercrime. To accomplish this, it is necessary to penetrate the company's IT equipment, which mainly consists of the databases with the personal information and financial information of customers.

Defending company information systems from cybercrime is one of the most important aspects of technology management. The theft of assets and loss of business caused by cybercrime is often in addition to reputation damage, which can create a negative impact on a company's stock price. Management, financial analysts, investors, and creditors are seriously concerned about this (Smith, Jones, Johnson, & Smith, 2019).

2.3. The Human Factor and Data Breach

As the volume of data is growing exponentially and data breaches are happening more frequently than ever before, detecting and preventing data loss has become one of the most pressing security concerns for enterprises (Cheng et al., 2017). Employees are the organization's strongest assets and factors, but they can also be its weakest link when it comes to data protection, particularly during times of

increase in mobility and accessibility. Trend Micro's (2018) research found that employees are the main cause of data breaches, despite the growing fear of cybercrime, and only 8% of the corporations surveyed indicated that external attacks were the main cause of breaches. The data breaching was also primarily caused by the loss of laptops or other mobile devices, 32% by third party error, and 29% by systems glitches, according to 35% of corporations. In spite of this, 56% of employees have provided information about sensitive business data on their smartphones, laptops, tablets, and other mobile devices. Approximately 19% of employees self-reported data breaches, and 56% of surveyed corporations found that data breaches are mostly discovered by accident. As a result of these employee practices, data breaches are the 10 most likely to occur: “1- Insecure wireless networks Using the same username and password for multiple websites or online accounts 2- Failing to delete unnecessary but confidential data from computers 3- Sharing passwords with others 4- Accessing the internet via unsecured wireless networks 5-The use of generic USB drives without proper encryption to store confidential information 6- The failure to notify organizations after losing USB drives containing confidential data 7- Failure to utilize the privacy screen when working on confidential company documents 8- Using a laptop that has excessively sensitive information when traveling 10- Using personal mobile devices to access the organization's network.”. As a result of the above discussions, organizations need to have cybersecurity policies and strategies. There are various types of attacks associated with different types of threats. There are several ways these can affect business information today, namely worms, viruses, denial of service, access, and reconnaissance. The most commonly encountered cybercrimes are crackers, scammers, phishing and hacking attacks (Zadig, 2016). A threat to the firm's assets may benefit certain individuals or organizations. Among these people might be

former employees or business partners. It may be caused by an employee who accidentally compromises the firm's data, it may be due to competitors attempting to gain economic advantage by infiltrating other profitable firms. Data breaches can result in financial losses for businesses, especially those which conduct their business online, so they will be liable for any costs incurred due to data theft. Furthermore, there are other costs associated with such incidents, such as losing a firm's reputation, and losing its customer base, as well as cleaning and running their affected systems, as well as damages sustained by other firms connected to the firm involved, fines for any other losses of personal data, and other costs. In addition to reputational damage and financial losses, the loss of sensitive information can have a detrimental effect on the long-term stability of an organization. Data leaks are typically related to employee or customer identity, intellectual property, and financial records (Cheng et al., 2017).

2.4. State of the art literature in Cybersecurity

2.4.1. Definitions and terms

Cybersecurity: what is it? Basically, cyber security is protecting a network's information from cyber threats, which essentially prevents vulnerable databases from being damaged or destroyed.

(Loi et al., 2019) Cybersecurity is generally understood as the protection an entity has from deliberate attacks, those involving human causes with malicious objectives.

Systems, networks, and data that are protected from cyberattacks are considered cybersecurity. Cybersecurity is comprised of technologies, processes, and controls. Depending on how it is implemented, cybersecurity can either be effective or

ineffective. An effective cybersecurity policy reduces the risk of cyber-attacks and prevents unauthorized use of systems, networks and technologies (Haapamäki & Sihvonen, 2019).

2.4.2. Cybersecurity Objectives

In cyber security, the primary goal is to ensure the attainment and maintenance of security properties of the organization and the assets of its users against relevant security risks. The term cybersecurity is often used to describe information security in an analogous manner; first, it ensures that private information remains confidential; second, it ensures that authorized users have timely access to information; and third, cybersecurity ensures that information is accurate, reliable, and valid (Haapamäki & Sihvonen, 2019).

To avoid cyber threats, every organization should implement a cybersecurity program or a cybersecurity strategy. This also applies to countries and jurisdictions, and hence, it was argued that it is essential for countries to publish national cybersecurity strategies (Haapamäki & Sihvonen, 2019).

A crucial component of any organization's cybersecurity policy is the ability to handle escalating cyber threats, as not only are individuals and corporations being attacked, but national security is also at risk (Mishra et al., 2022).

Atoum et al. (2014) stressed the importance of implementing cybersecurity in their study about cybersecurity implementation frameworks; first to identify potential threats earlier and mitigate the risks associated with government information systems and critical infrastructures. To help decision-makers take necessary actions when necessary, and to implement security solutions that involve a broad range of stakeholders, including citizens, businesses, and government agencies.

In Gcaza & von Solms (2017), cybersecurity contributes to the development of confidence between different stakeholders.

2.4.3. Cybersecurity Culture

With the rise of human factor attacks in recent years, the topic of security culture has dominated both practice and research. The term "cyber security culture" has been used more recently in this domain.

To minimize cyber risks from a human perspective, a cybersecurity culture must be promoted at an international, national, organizational, and personal level

As Al Shaikh (2020) pointed out, establishing a security culture within organizations goes far beyond the responsibilities of cybersecurity teams or cybersecurity communication managers. Each employee at every level must put in tremendous effort and invest heavily in this process. Building culture involves a high level of coordination between different campaigns and collaboration between internal and external stakeholders, according to the participants in his study.

As defined by Da Veiga (2016), cybersecurity culture refers to the way cyberspace is utilized from an international, national, organizational, or individual perspective in accordance with the attitudes, assumptions, beliefs, values, and knowledge of cyber users.

A security culture considers the social, cultural, ethical aspects of a user in order to change the overall security behavior. As defined by Gcaza & von Solms (2017), cybersecurity culture refers to “the intentional and unintentional ways in which cyberspace is utilized from the perspective of the individual, organization, or nationality, based on the attitudes, assumptions, beliefs, and values of the individual.”

Are there any factors that can affect the cybersecurity culture of an organization? Specifically, how much of an impact can such factors have on the cybersecurity culture within the organization?

Ultimately, managers are responsible for driving cybersecure behavior. Creating a cybersecurity culture (beliefs, values, and attitudes) is one way to accomplish this. As a result, both external factors beyond managers' control, and internal organizational mechanisms employed by managers, influence the culture.

2.4.3.1 Organizational Cybersecurity Culture

Cultures can differ significantly within and between organizations. They can bring out the best in people and create excellent environments for people to work in or they can bring out the worst in people and create dysfunctional environments filled with stress and tension. The importance of organizational measures in cybersecurity is increasing (Reegard et al., 2019). The concept of organizational culture is typically used by researchers to describe the culture of an entire organization or any unit within an organization (Warrick, 2017).

The concept of organizational culture refers to how the members of an organization understand the organization's unique cultural characteristics. Nabella et al., (2022) argue that the organizational culture refers to the values, beliefs, and shared norms that each member feels, thinks, shares, and embraces, as well as the habits all members of the organization follow. Those indicators include values, beliefs, rules, tolerance, results-oriented thinking, a focus on people, collaboration, teamwork, identity, stability, communication patterns, etc.

An analysis of organizational culture, national culture, and information security culture was conducted in order to develop a model of cybersecurity culture.

Huang & Pearlson (2019) drive employee behaviors to protect and defend the organization from cyber-attacks.”

This research focuses on the organizational cyber culture model presented by Huang & Pearlson (2019), which explains the factors that contribute to its development and how to measure it.

Those sections below illustrate some of the external/internal, behavioral factors that affect cybersecurity culture by exploring some of the motivations behind behavior.

2.4.4. Cybersecurity External Influences

The external influences that affect operations and success are factors beyond a company's control. It is possible to be affected by external factors such as economic recessions, government regulations, major lawsuits that damage a company's reputation or resources, acquisitions by another company, or natural disasters (Warrick, 2017). External influences can influence organizational cyber security culture in different way. Huang & Pearlson (2019) described the external influences that may affect cyber culture as an individual or organization's attitude, belief, and value towards cyber security. Reporting on cyber breaches in the public press, for instance, makes people more aware of cyber risks.

Organization culture can be significantly influenced by three external factors (Huang & Pearlson, 2019):

2.4.4.1 Societal Cybersecurity Culture

This refers to an organization's understanding of the cultural norms of its surrounding society. A person's perception of online threats may differ depending on his or her country of origin and culture. As an example, some countries place a high value on data protection. As a result, the beliefs of the organizations operating

in that country are likely to reflect the culture of that country. Similarly, some organizations operate in countries with a more laissez-faire culture, and we expect their cybersecurity cultures to reflect this.

Moreover, the external environment plays a major role in cybersecurity. For example, if an organization is located in a politically stable country with advanced technological capabilities, then its computer networks may not be localized and/or arbitrarily compromised. Nevertheless, if an organization is trapped in a volatile political environment accompanied by international hostilities, then various external motivations can lead to cybercrime (Shihan & Radif, 2022).

2.4.4.2. External Rules and Regulations

It encompasses the laws, guidelines, and regulations that are imposed by the government and other industry organizations. In view of the significant externalities associated with cyber security, development of cybersecurity policies by government agencies, or by powerful organizations such as supervisory authorities, can have a significant impact on the cybersecurity culture of an organization. In certain industries, such as financial services, we expect companies to have different beliefs and attitudes toward cybersecurity than organizations in other sectors.

The Federal Trade Commission and HIPAA regulatory agencies heavily involve private organizations in establishing current practices and standards of cybersecurity, including GrammLeach Bliley, HIPAA, and GrammLeach Bliley. As a result, state cybersecurity laws — a form of disclosure-based regulation that in fact achieves directive regulation — detail specific standards that were not developed in consultation with the industry (Thaw, 2013).

Effective cybersecurity regulation is becoming increasingly important to counter threats as a regulatory object. Cybersecurity has unique characteristics and challenges that it presents, and their identification will assist in establishing a set of key elements cybersecurity regulations need to adhere to for effective implementation (Calliess & Baumgarten, 2020).

It is essential to have effective cybersecurity regulations that cover new technologies as well as third-party cyber risks. The regulations must also establish the conditions that financial institutions can enter into outsourcing agreements with third-party service providers, as well as the requirements regarding the management and monitoring of the risks associated with such agreements. Cybersecurity regulation must pay particular attention to risk prevention because cyber risks are rapidly evolving and technical developments and threat scenarios cannot be predicted. (Calliess & Baumgarten, 2020).

2.4.4.3. Peer Institutions

Describes the pressure that managers in an organization feel in response to the actions taken by their peers. Institutional mimicry theory provides some support for this construct. The institution mimicry theory supports this concept. Since cybersecurity is a relatively new threat with many uncertainties, managers are often looking to their peers for guidance. It is possible to learn what options their peers have adopted through trade associations, conferences, and even simple social situations. To stay competitive, organizations need to adopt strong cybersecurity practices that match their supply chain requirements. Tuttle & Dillard (2007) describe competitive isomorphism as a drive to improve efficiency and effectiveness.

2.4.5. Cybersecurity Internal Mechanisms

It is important to note that there are a number of internal factors that could affect culture. These factors include organizational structures, processes, systems, budgets, and leadership styles, etc. (Warrick, 2017). In an organization, the most important factors affecting its cybersecurity culture are those that originate from the management or can be controlled by managers. In support of this, Uchendu et al., (2021) claim that top management support, policies and procedures, and awareness is essential for shaping cyber security culture. A culture is formed by the beliefs, values, and attitudes of the employees, but they are created by management levers or organizational mechanisms created by the leaders of the organization. The figure 1 illustrates how managers can influence cybersecurity culture using six managerial levels. These levels allow managers to make decisions, which in turn drive (and can drive) culture.



Figure 2: Huang and Pearlson (2019) Organizational Mechanisms for Cybersecurity

2.4.5.1. Cybersecurity Culture Leadership

refers to the Assigning an individual or team to build a cybersecurity culture. Cybersecurity culture should be cultivated by this leader, who has direct authority

over the process. CISOs are often looked to drive change in organizations, but someone other than the CISOs, who have a very large agenda covering all aspects of cybersecurity culture, ought to take on this task. It will be difficult for the culture to be built without a leader specifically responsible for it, which will cause the activities to be carried out haphazardly and sometimes skipped altogether.

Based on a study conducted by Kark, White and Briggs (2015), there are four factors that influence CIO performance, including "business priorities, leadership and talent, relationships, and investment priorities. Based on these key elements, Deloitte University Press surveyed 1,271 participants in 43 countries across top industries, 19% of whom were financial sector workers. According to the survey, CIOs and top IT executives of leading organizations around the world have all identified their top business priorities as directly related to their business hub; according to the CIO survey, these five business priorities define the context in which CIO priorities are most valuable both today and in the future. Only 18% of investment priorities were dedicated to cyber security. Consequently, financial service CIOs rank cybersecurity at the bottom of their priorities. This could be due to the importance of achieving other priorities, or maybe they do not generate profit or it may be that these duties are shared with other top management. It is also possible these CIOs are lacking CSA and training. Cybersecurity is the significant backbone that can affect and inspire all the five top business priorities, so it could be risky to disregard it.

Employees and senior managers play a key role in determining organizational performance and strategy (Sebola et al., 2020).

Having studied the themes, it becomes evident that healthy cultures are largely the result of effective leaders and managers, whereas unhealthy cultures are largely the

result of ineffective leaders and managers. (Warrick, 2017). Additionally, Warrick outlined the following guidelines for building and sustaining cultures:

1. Ensure strategy and culture are top priorities for leaders.
2. Understand the current culture clearly.
3. Engage employees in cultural ideals by identifying, communicating, and educating them.
4. Model the behaviors you want to see.
5. Develop a culture-fit recruiting and development process.
6. Ensure that strategy and culture are aligned.
7. Practices and behaviors that are desired should be recognized and rewarded.
8. Reinforce culture through symbols, ceremonies, socialization, and stories.
9. Appoint a team to manage the culture.
10. Manage and monitor the culture.

Further, Warrick (2017) distinguishes between high and low performance cultures in his research, as shown in the table below:

High Performance Cultures	Low Performance Cultures
Leaders are skilled, admired, and build organizations that excel at results and at taking excellent care of their people and their customers	Leaders provide minimal leadership, are not trusted and admired, and do little to engage and involve their people
Clear and compelling vision, mission, goals, and strategy	Vision, mission, goals, and strategy are unclear, not compelling, not used, or do not exist
Core values drive the culture and are used in decision making	Core values are unclear, not compelling, not used, or do not exist
Committed to excellence, ethics, and doing things right	Lack of commitment to excellence, questionable ethics, and a reputation for doing what is expedient rather than what is right
Clear roles, responsibilities, and success criteria, and strong commitment to engaging, empowering, and developing people	Unclear roles and responsibilities and little interest in fully utilizing and developing the capabilities and potential of people
Positive, can-do work environment	Negative, tense, stressful, and/or resistant work environment
Open, candid, straightforward, and transparent communication	Guarded communication, reluctance to be open and straightforward, and consequences for saying things leaders do not want to hear
Teamwork, collaboration, and involvement are the norm	Top-down decision making with minimal teamwork, collaboration, and involvement
Emphasis on constant improvement and state-of-the-art knowledge and practices	Slow to make needed improvements and behind times in knowledge and practices
Willingness to change, adapt, learn from successes and mistakes, take reasonable risk, and try new things	Poorly planned change, resistance to change, minimal learning from successes and mistakes, and either risk averse or risk foolish

Table 1: A comparison of high and low performance cultures adapted from Warrick (2017)

2.4.5.2. Performance Evaluations

Describes the inclusion of cybersecurity compliance measures and behaviors in formal evaluations of employees. Using expectation theory, managers use performance evaluations to clarify what behaviors are required, desirable, and unacceptable. For example, it might be unacceptable for employees to hand out system passwords to vendors without **specific** approval from upper management. Furthermore, managers might include the results of their regular phishing exercises in employee evaluations. Employees will be aware of the organization's ability to observe cybersecurity behaviors through performance evaluations. This can have a positive impact on their values as a result.

Evaluation of employee performance aims to determine whether the organization meets its goals by assessing individuals' contributions to the organization, and whether the organization meets its goals by evaluating their performance against organizational goals. In general, performance evaluations serve two purposes: first, to reward employees who meet organizational goals and second, to identify which goals have not been met and develop action plans to achieve them in the future (Islam & Rasad, 2005).

2.4.5.3. Rewards and Punishments

Cybersecurity behaviors have managerial impacts. Individual decisions are highly influenced by the design of rewards and punishments within many different contexts, according to the rational choice theory, the deterrence theory, and the protection motivation theory. Employees with exemplary behavior may receive rewards, proclamations, and certificates, whereas those with exemplary behavior may receive reprimands, remedial training, or even be terminated. It is important that rewards and punishments are matched to the severity of the behavior for them to be most effective. For instance, failing a phishing test is probably not ground for firing an employee, but in one company Huang and Pearlson (2019) studied, an employee was fired for repeatedly failing phishing exercises. In response to concerns over his actions, management warned him several times, then let him go.

A culture can also be built by rewarding, recognizing, and valuing behaviors that promote it. Leaders talk all kinds about the type of culture they want, but in the end, employees will respond to the behaviors they see rewarded, valued and recognized. As a result, leaders must be aware of the behaviors they are reinforcing. According to some scholars, the crash of the NASA space shuttle Columbia and Challenger explosions in space were the result of NASA's shift from rewarding

space safety and technical brilliance to valuing efficiency and reusing space shuttles (Warrick, 2017). (Warrick, 2017).

2.4.5.4. Organizational Learning

Explains how the organization obtains and retains cybersecurity expertise. Organizing to learn can be defined as transforming the organization continuously by utilizing learning processes exclusively used by its individuals, groups, and systems so that it becomes increasingly satisfying to its stakeholders. Organizational learning can be a key component of managing continuous change in cybersecurity. A few examples of organizational learning for cybersecurity include mentors who help individuals build skills, processes that promote information sharing, or consultants who add new insight.

For organizational learning to occur, individual members must be embedded in a supra individual repository of knowledge that they acquire. As a result, knowledge accumulated by individual members should be embedded in the organization so that it can be accessed by all members, regardless of whether they remain members or not. The process of organizational learning is divided into three phases: creating, retaining, and transferring knowledge; as an organization learns from experience, new knowledge is created within the organization (Argote, 2011).

Organizational learning (OL) enables organizations to transform individual knowledge into organizational knowledge, and it is also perceived as a management task involving planning and controlling. In addition to creating, capturing, and internalizing organizational knowledge, it focuses on organizational strategic planning (Basten & Haamann, 2018).

2.4.5.5. Cybersecurity Training

This category refers to courses and exercises that focus on developing cybersecurity skills and knowledge. Educating users about security and training insiders to take on security roles are all necessary elements of training that fosters information security awareness. Several organizations require employee training on cybersecurity practices annually, as noted in Huang & Pearlson's (2019) research. In their conversation with cybersecurity teams, Huang & Pearlson (2019) conclude that a single onboarding training course is not enough to sustain long-term behaviors; proactive, diversified training is required.

As a result of security awareness, organizations minimize security incidents, develop new application systems faster, and ensure controls are consistently implemented across their information systems (Wood, 2008). A CSA program, according to Krutz & Vines (2001), aims to train users about their responsibility for maintaining the privacy, accessible, and reliable data stored by their organization. In addition, Johnson (2016) states that lack of CSA across workforces has been documented as a major barrier to success for any cybersecurity position. Several countries have developed security programs and campaigns aimed at increasing awareness of cyber security. In Australia, different training and education programs have been developed by working with foreign governments and institutions, in order to raise awareness about this major issue (Bada et al., 2014). Cyber security month is celebrated in the USA every October, where professional guests are invited to speak at competitions, discussions, and campaigns (Obama, 2010; Aloul, 2012). The Canadian government, private and public sectors as well as its community have come together to develop a campaign called "get cyber safe" to educate their people about cyber security (Bada et al., 2014). In Japan, they celebrate the cyber security awareness campaign every October to remind them of

cyber security's importance (Beuran et al., 2016). The Government of Qatar has collaborated with some of its international partners in order to raise awareness, identify cyber threats, and coordinate its actions in order to improve cyber security worldwide. Qatar has also established an award program that aims to reward cyber security experts (AlHamar, 2016). As part of the Gulf Cooperation Council (GCC), Bahrain has been home to a cyber-security lab since 2017. The purpose of this lab is to raise awareness about cyber security and develop solutions to overcome the increased number of cyber-attacks occurring in the Middle East and North Africa region (MENA). Also in 2017, Bahrain held a three-day cyber-security exhibition, 16th - 18th May, as part of its efforts to increase awareness and educate more people about this emerging problem (Zafran, 2017).

2.4.5.6. Communications Channel

It includes a variety of methods and networks for communicating coherent, well-designed cybersecurity messages. Communication in business requires the right information being heard by the right person at the right time on the right channel to be successful. Some things may work for one person and not for another. Cyber incidents must be reported, dynamic cyber information shared, and even potential vulnerabilities must be identified through formal and informal channels. Some organizations, for example, use cybersecurity-based marketing campaigns to keep employees informed about cybersecurity issues. The first few minutes of every company meeting should include a short cybersecurity message as an example.

2.4.5.7. Cybersecurity Budget

Cybercrime losses can be prevented by determining how much businesses are willing to spend on cyber security. Among the possible losses are repair costs, recovery costs, lost business, and possible closures. Every year, cybercrime costs

grow. Cybercrime is often unreported, so estimating losses from cybercrime may be difficult. It is estimated that cybercrime costs US businesses over \$400 billion annually, including direct damage and disruption caused by post-attacks (Smith, Jones, Johnson, & Smith, 2019).

2.4.6. Beliefs, Values & Attitudes

In Huang & Pearlson's (2019) model, cybersecurity culture was modeled on organizational culture. Cybersecurity culture plays a central role in Huang & Pearlson's (2019) model. There are unwritten rules that everyone knows but few are capable of articulating: values, attitudes, and beliefs. Nevertheless, leaders, groups, and individuals within an organization can demonstrate them through the actions they take.

There are nine constructs that make up culture at these three levels of the organization, as shown in Figure 2.

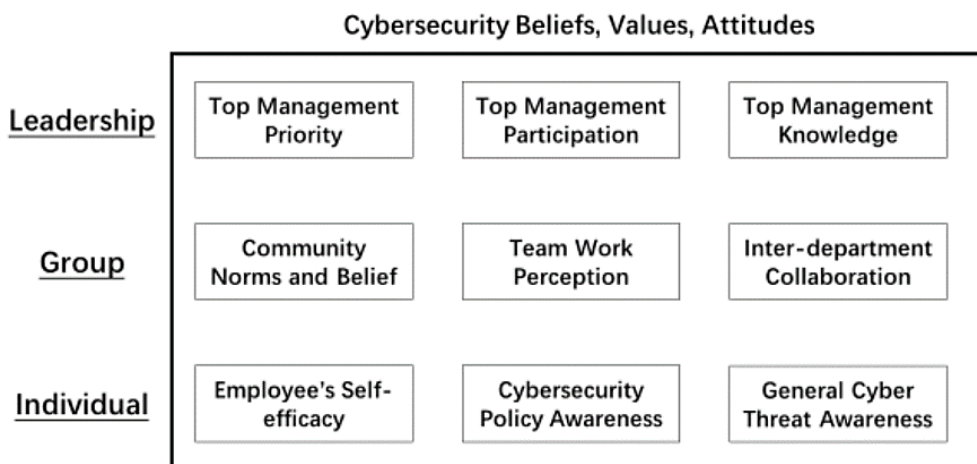


Figure 3: Adapted from Huang & Pearlson (2019) the three organizational levels of cybersecurity culture

2.4.6. Cybersecurity Employee Behavior

The performance and efficiency of an organization depends on the behavior of its employees. Organizations differ in their use of technology. In a business environment, an organization's ability to thrive depends largely on the acceptance, rejection, and adaptability of employees to new technology. By using technology, organizations are able to improve their economic efficiency, make work processes easier, quicker, and more efficient. Agboola et al., 2019 have also found that technology use greatly influences employee behavior.

Throughout this paper, we will focus on cybersecurity technology. It is more than just a technical issue when it comes to cybersecurity, so organizations must rely on the behavior of their employees to prevent and deter cyber-attacks. As a result, employee behavior is ultimately the determining factor in the creation or reduction of cyber-based vulnerabilities. As a result of a cybersecurity culture, there are two types of behaviors: behaviors within the role and behaviors outside the role (Huang & Pearlson, 2019).

Behavior can be considered a response to a situation by an individual. The way an individual behaves is not simply influenced by one variable, but also by societal norms, values, and their desire to fit in; knowledge and awareness of cyber-risks.

Trying to explain human behavior is a challenging task. Ajzen's TPB model is the most popular and useful explanation for human behavior. A variety of studies (sociology, psychology, social psychology) have used the TPB to provide explanations for human behavior (Emekci, 2019).

TPB is an expectancy value model. According to TPB, human behavior is affected by three factors: behavioral (linked to intention), normative (societal or group

behavior), and control beliefs (related to performance and self-efficacy). As a result of these three factors, behavioral intentions may be determined, but not necessarily translated into behavioral actions. A crucial element of planned behavior theory is a person's intention to perform a specific behavior. A person's intention is believed to represent their motivation behind a behavior; it measures how much effort they will exert to perform a behavior (Ajzen, 2020). Nonetheless, people do not always follow through on their intentions. Therefore, we cannot say that intentions always cause people to behave in a way they intended

2.4.7. Technology Acceptance Theories

A variety of theories and models have been developed to explain patterns of human adoption and use of new technologies due to the complexity involved in predicting human behavior. As technology has reshaped every aspect of life, technology acceptance research has matured over the past two decades. Several theoretical models have been developed to explain end users' acceptance behavior. Consequently, technological innovation acceptance requires psychological models and theories to explain and rationalize whether users benefit from new devices. Several models of technological acceptance have been developed, each with its own characteristics.

In order to understand technology acceptance studies, it is important to know what theories or models were used to conduct these studies. Therefore, in the following subsections, we discuss popular models and theories related to technology acceptance.

1. Theory of Reasoned Action (TRA) (1975): Using perception, norms, and attitudes to predict behavior related to the intentions of making a decision, it explains how a person might react as a result of that decision.
2. Social Cognitive Theory (SCT) (1986): Developed by Albert Bandura in 1986, the social cognitive theory (SCT) proposes that behavior is acquired and maintained by considering the social environment in which it is developed. In their models, both the theory of planned behavior (TPB) and the technology acceptance model (TAM) assume unidirectional causal relationships between the main variables.
3. Technology Acceptance Model (TAM) (1986, 1989): Perceived usefulness and ease of use are two important factors in this theory, attitude towards using a new system is a determinant of future behavior or causes of intentions that eventually lead to certain behaviors. As opposed to TRA, the TAM does not include subjective norms due to the poor psychometric results it generates (Davis et al., 1989; Wu et al., 2011), so researchers have used it to analyze the adoption of various technologies in the ICT field, making it the most important theory in this field.
4. Theory of Planned Behavior (TPB) (1991): In 1991, Ajzen developed the TPB as an extension of TRA, adding the additional determinant of intention perceived behavior control to alleviate some of the drawbacks of TRA.
5. Model of PC Utilization (MPCU) (1991): Thompson et al. (1991) developed a model that predicts PC usage behavior, identifies six factors associated with technology acceptance, respectively, job fit, complexity, long-term consequences, affect toward use, and social factors.
6. Motivation Model (MM) (1992): Davis et al. (1992) applied the motivation model to the study of ICT adoption and use, positing that an individual's

behavior is determined by intrinsic and extrinsic motivations, and furthermore by psychological factors.

7. Combined TAM – TPB (1995): Attitudes can be decomposed into perceived usefulness, perceived ease of use, and compatibility, whereas peer influence and superior influence the normative belief structure, whereas self-efficacy and facilitating conditions influence the control belief structure.

8. Innovation Diffusion Theory (IDT) (1995). Innovation diffusion theory was developed by Rogers in 1995. Innovation refers to the idea, process, object, or practice that can be considered as being new, while diffusion refers to the method by which it becomes part of society. A relative advantage, compatibility, complexity, trial ability, and observability are five of the determinants of the rate at which innovations are adopted and accepted, according to this theory.

9. Extension of TAM (TAM2) (2000): Venkatesh & Davis (2000) added social influences and cognitive instrumental processes to the original TAM to form the TAM2. Cognitive instrumental processes are influenced by subjective norms and images, while social influences are influenced by job relevance, output quality, results demonstrability, and perceived ease of use. All of these additional elements are believed to influence technology acceptance, which is directly determined by perceived ease of use in TAM2. Davis argues that behavioral intentions to use can be influenced by both experience and voluntariness in this model, so subjective norms are not considered in the TAM. However, in extending TAM, Venkatesh & Davis (2000) reexamined these variables.

10. Unified Theory of Acceptance and Use of Technology (UTAUT) (2003): Venkatesh et al. (2003) combined the different models and theories of

technology acceptance into a unification theory. According to their model, eight technology acceptance theories and models were integrated into one unification theory: TRA, TAM, motivation, TPB, combined TAM-TPB, PC utilization model, innovation diffusion theory, and social cognitive theory. In the UTAUT model, four main variables are responsible for usage and intention: performance expectancy, effort expectancy, social influence and facilitating conditions. These factors are moderated by four variables: gender, age, experience, and voluntariness.

11. Technology Acceptance Model (TAM3) (2008): Venkatesh & Bala (2008) modified the TAM by giving the dimension 'perceived ease of use' a higher level of significance and adding computer self-efficacy, perception of external control, computer anxiety, and computer playfulness. The TAM3 was developed on the basis of four classifications that Venkatesh and Bala claim are a synthesis of previous research on TAM (2008), which adds two additional adjustment variables, which are perceived enjoyment and objective usability. This model identifies the perceived ease of use of computers as a function of four factors: computer self-efficacy, computer playfulness, computer anxiety, and perception of external control. Subjective norms, job relevance, results demonstrability, and image determine perceived usefulness; however, one criticism of the model is that there are too many variables and relationships between them.

12. Extending Unified Theory of Acceptance and Use of Technology (UTAUT2) (2012): Venkatesh et al. (2012) have developed an extension of the unified theory of technology acceptance and use. A consumer use context was highlighted in this model through the addition of three additional variables: hedonic motivation, price value, and habit, in addition to the independent

variables of UTAUT. To tailor UTAUT to consumer technology use contexts, Venkatesh et al. have integrated these three independent variables into UTAUT, in addition, they have combined these three salient constructs. This theory expands the general framework with regard to technology use by including age, gender, and experience as moderating variables, but it does not consider voluntariness.

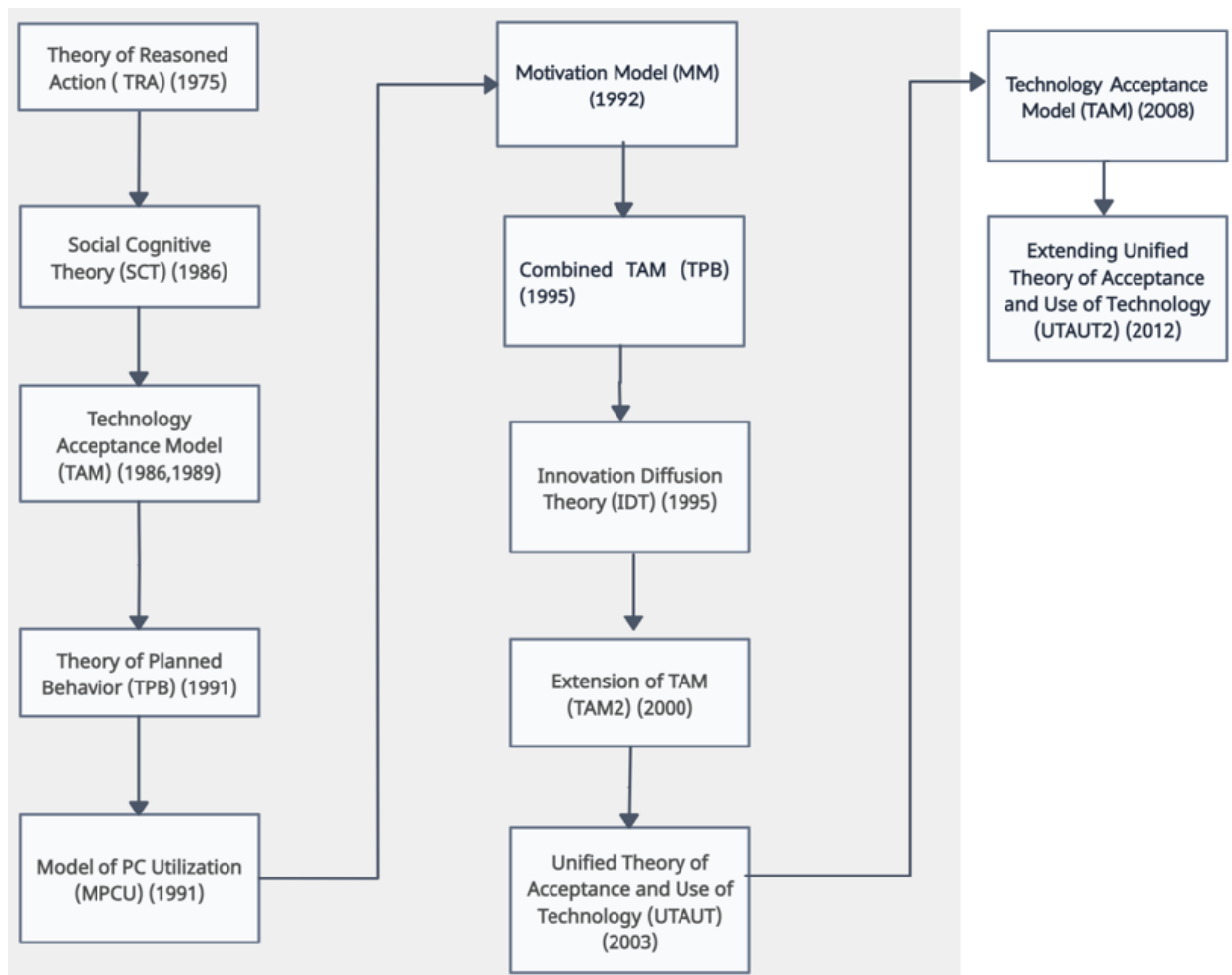


Figure 4: A Chronology of Acceptance Models Development

We can conclude that the success of new technology depends on user acceptance, therefore, uncovering the antecedents of technology use is an essential step in overcoming the lack of user acceptance.

2.5. Theory of Acceptance and Use of Technology (UTAUT2)

Identifying the factors that influence the adoption, acceptance, usability, and use decisions of technologies is crucial for technology practitioners and manufacturers. Users, technology, and the environment in which the technology is used are typically taken into account when analyzing these decisions. Over the past three decades, researchers have examined these features using the unified theory of acceptance and use of technology (UTAUT) and the technology acceptance model (TAM).

The UTAUT has studied learning management systems, mobile learning, instructional devices, online collaboration tools, and educational services in many of its studies. UTAUT is one of the most widely used theoretical frameworks for predicting what systems will be used for by individuals. It has been widely used to study new technological systems and has proven to be a robust predictive model. The purpose of UTAUT is to emphasize the importance of utilitarian value and was developed to ensure employee acceptance and use. UTAUT has been used in a number of empirical studies to investigate the relationship between situational factors and technology use behavior since it was developed.

The adoption of technology consists of at least eight competing models. The theories are: the theory of reasoned action (TRA), the technology acceptance model (TAM/TAM2), the theory of planned behavior (TPB)/decomposed TPB, the

combined theory of TAM and TPB (CTAM-TPB), the motivation model (MM), the model of PC use (MPCU), insight diffusion theory (IDT), and social cognition theory (SCT). A theory of acceptance and use of technology was proposed by Venkatesh, Morris, Davis, and Davis (UTAUT) in 2003 (Chang, 2012).

Venkatesh et al. (2003) finds that UTAUT can be moderated through four factors, namely performance expectancy (PE), effort expectancy (EE), social influence (SI), and facilitating conditions (FC). It is possible for these variables to have an impact on consumers' use intention and behavior when it comes to technology. As well as gender, age, experience, and voluntariness, four other variables moderate the relationship between independent variables and dependent variables.

A total of eight IT acceptance models were incorporated into Venkatesh et al. (2003)'s Unified Theory of Acceptance and Use of Technology (UTAUT). According to the findings from the Hong Kong research conducted by Venkatesh et al. (2012), the UTAUT model has been modified. The UTAUT model was modified by Venkatesh et al (2012) to include three new constructs. Hedonic motivation (intrinsic motivation) is the first construct. Another important factor is the price, where consumers must pay for devices and services. The third construct is habit. Using the proposed additions to UTAUT2, Venkatesh et al. (2012) found significant changes in behavioral intention and technological use based on UTAUT2's proposed additions.

Consequently, in search of an appropriate model that covers almost all constructs determining Bahraini government employees' intentions and adoption of cybersecurity, the UTAUT2 has been chosen as the theoretical foundation for proposing the conceptual model utilized in this study.

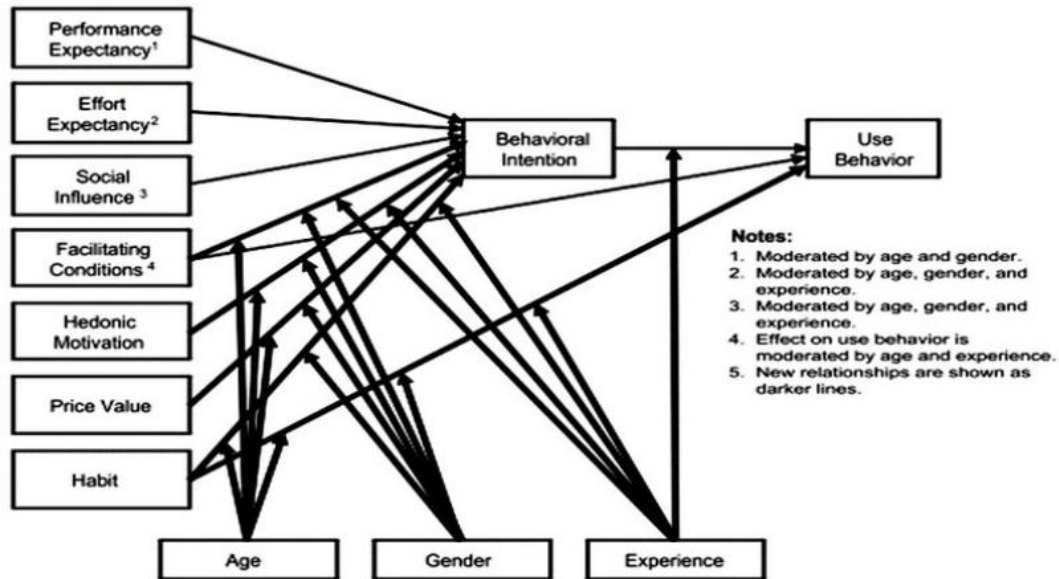


Figure 5: Conceptual Framework of the UTAUT2

2.6. Limitation of UATUT 2

Despite its great accomplishments in shaping understanding of technology use behaviors, UTAUT2 has several limitations. A limitation of current technology acceptance models (e.g., TAM and UTAUT) is the lack of several important attributes associated with human behavior and technological design. Additionally, both the TAM and UTAUT do not include many of the important features of technology acceptance because they are structurally linearly explanatory. In turn, this undermines their effectiveness and makes them less practical (Alwabel & Zeng, 2021).

UTAUT unites factors and functions of TAM with those of a number of other popular IT adoption models, making it highly complex, so it is difficult to assess whether it can be applied to actual IT adoptions (Boonsiritomachai & Pitchayadejanant, 2017). Aside from this, UTAUT produces meaningless output values (R^2) that range from +1 to -1 inclusive. Therefore, UTAUT cannot be used

to support end users' technology decision-making. In this regard, it is imperative to develop a prediction model of technology acceptance that defuzzied these output values and categorizes technologies as usable, likely to be usable, or unusable. A major limitation of the current UTAUT is that it is structurally linearly explained and excludes many important features of technology acceptance. As such, the UTAUT undermines its effectiveness and impacts its practicality (Alwabel & Zeng, 2021).

It is therefore necessary to develop an explanatory and predictive model that can incorporate both linear and non-linear influences on technology acceptance. In addition to being aligned with the current UTAUT, such a model should be capable of including new features of technology acceptance

In this research, it is believed there is a need to introduce methodological advancements, such as ML, that will eliminate the limitations of UTAUT as described above.

2.7. Machine Learning in Technology Acceptance

In the field of multidisciplinary technologies, machine learning has emerged with the rise of big data technologies and high-performance computing to provide new opportunities for data intensive science.

Machine learning (ML) is used to teach machines how to handle the data more efficiently. Sometimes after viewing the data, we cannot interpret the extract information from the data. In that case, we apply machine learning. With the abundance of datasets available, the demand for machine learning is inc rise (Alwabel & Zeng, 2021).

Since machine learning techniques are capable of predicting a target factor from embedded parameters, many researchers have used ML to determine a target factor. The acceptance of technology and machine learning have also been combined in numerous researches, yet some of these studies have compared technology acceptance with machine learning results. The two strategies are popular and efficient in analyzing a symmetrical system while maintaining symmetry (Chauhan et al., 2021). An analysis of major factors that encourage mobile games industry growth was conducted by Chauhan et al., (2021). This study utilized machine learning to identify the key mechanisms involved in evaluating online games complex problem. As part of the analysis, two phases were utilized: the first phase involved using a TAM Model, which is an efficient statistical solution to problems, and the second phase involved machine learning (ML) techniques, such as SVM, logistic regression, etc.

Almaiah et al. (2021), rely on machine learning prediction to predict future events. They proposed a hybrid model combining the TAM model with new constructs from the UTUT model in order to understand the main factors influencing the acceptance of mobile learning applications by combining the TAM model with new constructs from the UTUT model in order to understand the main factors influencing the adoption of mobile learning applications. The proposed model was analyzed using machine learning algorithms to determine the relationships among the constructs.

Also, Al-Marooof et al., (2020) conducted a study in order to understand the factors influencing the acceptance of WhatsApp stickers by students, and this study integrates the TAM theory with the U&G theory in order to identify the factors that influence students' acceptance of these tools. Through the use of machine learning

algorithms, this study analyzes the hypothesized relationships among the constructs in the proposed theoretical model through the application of TAM and U&G for the purpose of predicting student acceptance of stickers.

Overall, Machine learning is important both for exploring and answering the fundamental scientific and engineering questions and for producing highly practicable software for a variety of applications (Jordan & Mitchell, 2015).

2.8. Cybersecurity working group in the GCC

Cybersecurity is a process for safeguarding computers, servers, networks, and data from unauthorized access, destruction, and attack. Nonetheless, safeguarding financial data, intellectual property, and reputation should be an essential part of an organization's business strategy. As businesses and governments use cybersecurity, their goals are not only to protect confidential information, but also to ensure the availability of the information and maintain its integrity (Alawi, 2006).

According to Al-Alawi (2006), information security is crucial to the national security of any nation; many countries have developed a comprehensive framework for ensuring cyber security. A technological boom in the USA has led to security challenges for the nation and its citizens, so it must work to prevent the illegal use of information by ensuring the security of information through cybersecurity, which depends on technical and legal resistance.

A GCC country's liquid capital, oil prosperity, and cultural position make them attractive targets for cybercrime and attacks. Responses to cyber threats by GCC countries have major implications for the global economy. In 2012, for instance, a virus known as Shamoon infected about 30,000 of the company's workstations at ARAMCO, a state-owned oil company in Saudi Arabia. This had a significant

impact on the Pentagon's decision to develop a highly effective cyber security strategy within the United States (Bronk & Tikk-Ringas, 2013). Globally and in the GCC, this was the most horrific cyberattack in modern history. Due to an unaware computer technician opening a scam email and clicking on a bad link, flickering screens and disappearing files occurred, wiping and destroying more than 30,000 computers and causing the company to suffer a significant loss. As Raiu et al. (2017) indicate, Shamoon of 2012, the most mysterious wiper of all time, returns in a new version called Shamoon 2.0 or StoneDrill. In November 2016, it targeted a number of critical and economic sectors in Saudi Arabia.

According to an interview published in Infosecurity (2014) with General Alexander, former Chief of the United States Cyber Command and Chief of the National Security Agency's Central Security Service (CHCSS), the Saudi Aramco attacks have "severe implications for the safety of critical infrastructure networks".

As a result of the attack against Aramco, the United States military helped the company increase its cyber security awareness. After it was hacked, it lost 15 million dollars. In the neighboring countries, United Arab Emirates has increased security, and Qatar has started an investigation into cybercrime. As a result, the GCC countries have been providing trainings and seminars to increase the level of awareness of cybersecurity in their countries. With the support of the United States, they have also strengthened the Saudi government bodies to ensure the security of data. In The GCC's study by Hoffecker (2017), their key objectives are to increase awareness of cyber security, provide education, and increase their capability.

GCC efforts have been centered on improving their cyber security systems and approaches as a result of high numbers of cyber-attacks. In addition to energy and

water security, cyber-attacks and cybersecurity are among the major challenges facing the GCC. With this in mind, the Cybercrime Investigation Center and the Information Security Center were launched for the purpose of protecting critical technological data and information (Kshetri, 2016).

After the first GCC-USA summit in May 2015 at Camp David, USA, a cybersecurity working group was established to enrich security cooperation with the U.S.A., especially in the area of cyber security. On April 21, 2016, the second summit was held in Riyadh, Saudi Arabia (Bizbahrain, 2015; White House, 2015; White House, 2016). Moreover, Wahba (2016) asserted that cybersecurity was vital to current and future collaborations. Hence, the importance of developing cyber-talent and skills in GCC countries should not be underestimated. As part of our rapidly developing economy and the age of information, the UAE has taken a key leadership role in preparing young Emiratis to compete at a global level in technological fields and disciplines. In a collaboration with Khalifa University, the Arab Gulf States Institute in Washington and Raytheon, to improve cybersecurity, have provided government representatives, educators and businesses at the UAE Security Forum in Abu Dhabi in order to improve cybersecurity. As part of the project, the university will dialogue with major academic institutions, government officials, and industry leaders about “ways to bridge the gap in cyber curriculum and cyber training programs”.

2.9. Status of Bahraini Cybercrimes

With a superior telecommunication infrastructure and a number of positive developments, Bahrain is considered the banking hub of the MENA region, and its revenues are increasing because of the huge increase in the use of

telecommunications technologies such as Internet and mobile technology in recent years. According to Internet World Statistics (2017), the Middle East has a 58% Internet penetration rate, the world average is 51.7%, and the rest of the world has a 51.1% Internet penetration rate. According to the Oxford Business Group (2015), Bahraini legislation related to cybercrime consists primarily of the Constitution, the Penal Code, the Telecommunications Law, and the Central Bank of Bahrain Law. In light of the growing cyber threat and the need to modify the current law, Bahrain will introduce a new cybercrime law once it has been approved by the Shura Council, which will be built on the cybercrime convention of 2001, in addition to other international laws. It is possible for cyberattacks to originate from anywhere in the world, and Bahrain would benefit from modeling its new law on the Convention by being concise, more consistent, and able to rely on assistance from member countries in investigating and prosecuting cybercrime. As part of the cybersecurity tasks to be undertaken in Bahrain soon, the Information and e-Government Authority is also noting how many cybersecurity tasks will be carried out there. Further, CSA campaigns have already been launched by the government and organizations in the country to explain why cybersecurity is necessary to protect against any online threats and risks, as well as the need for the right infrastructure to prevent data breaches in the government and organizations. The government, however, estimated it would take four years to hire and train this cybersecurity task force (TradeArabia, 2014; Bizbahrain, 2015).

Bahrain has established a cybersecurity laboratory, according to Whelan (2017). A laboratory like this is a great way to raise the awareness of cyber-attacks in the Middle East and motivate people to come up with the best solutions to them. As a part of the lab, training sessions are provided to increase cyber security awareness in the Middle East.

According to Al-Maskati (2016), Central Bank of Bahrain prioritizes cybersecurity and implements three steps to strengthen it:

- “1) Developing cybersecurity capabilities within the financial sector through cooperation and sharing of information
- 2) Establish policies that ensure our financial institutions make cybersecurity a priority
- 3) In the event of a cyber-threat or incident, be prepared to respond quickly”

As for Bahraini banking, Abdulkareem (2012) reported that the Bahraini banking sector receives about 2,000 to 3,000 threats a month regarding cyber security risks. As part of their security audits, the bank regularly inspects their systems and uses antivirus protection tools.

Cyber-attacks and security are not yet well dealt with in Bahrain, with only 20% of companies prepared to handle them. Despite this, the government is working hard to provide protection against cybercrime and attacks. It was, however, necessary for HM the King Hamad bin Isa Al Khalifa to issue the Royal Decree No. because of an increase in cybercrime in Bahrain, and for the Kingdom's importance in the matter. Bahrain's Ministry of Interior has established a Cybercrime Directorate (Official Gazette, 2011).

2.10. An Overview of Banking Sector Importance

It is widely acknowledged that 2016 was a year of innovation that brought secure cloud computing to the banking sector, resulting in improved challenges. However, the advent of Artificial Intelligence (AI), biometrics, and hard-hitting firewalls does not guarantee that they will be hack-proof. As outlined by Vij (2016), a Russian cybersecurity organization shook the world by attacking more than 100 banks

worldwide with cyberattacks that resulted in the theft of one billion US dollars, in addition to the robbery of \$81 million at Bangladesh Central Bank. The banking sector has suffered over \$400 billion in losses a year as a result of these highly sophisticated planned criminalities, Vij said, citing the Federal Financial Institutions Council. In 2015, cybercriminals robbed \$40 million from only 12 debit card accounts via an ATM attack. In the past, both HSBC and NatWest sites were concerned after being targeted by hackers.

Considering the cost of cyberattacks to businesses in 2015, according to Raytheon & Websense (2015), the financial sector is more cautious than other organizations. In comparison with any other industry, the financial sector has to deal with 300% more cyber-attacks than any other, making it the most frequent target. As stated by Vij (2016), many leading banks partner with universities and research centers to detect and combat cybersecurity threats. This continuing investment not only benefits the bank but also encourages customer loyalty. Due to a series of attacks, the Royal Bank of Scotland has already committed hundreds of millions of pounds to software and hardware, and J.P Morgan doubled its cybersecurity budget to \$500 million. Further, this implies that banks need to improve their risk management plans and strategies, and to invest more in CSA and training: “becoming well-informed may be the best defense against criminal plots”. As cybercrime is kept very confidential in GCC countries (Morgan, 2016), no study has been conducted or a cost estimate has been found for cybercrimes in the GCC countries.

2.11. Research Gap

Previous section's literature was gathered through secondary methods of research, such as research papers, journal articles, online articles, books, government

records, official websites, and statistical databases. There is, however, insufficient data about how cybersecurity culture affects employee behavior in Bahrain in all these sources. Nevertheless, all these data relate to the wide-spread knowledge on the topic of this study worldwide. A major gap in the literature review is the lack of credible data on the impact of cybersecurity culture on employee behavior in Bahrain.

Specifically, this study examines the effects of cybersecurity culture on employee behavior in Bahraini banks.

Several gaps have been identified in literature that must be closed both in cybersecurity culture, employee behavior, and technology adoption in the conviction- and assurance-based economy to build a successful digital institution.

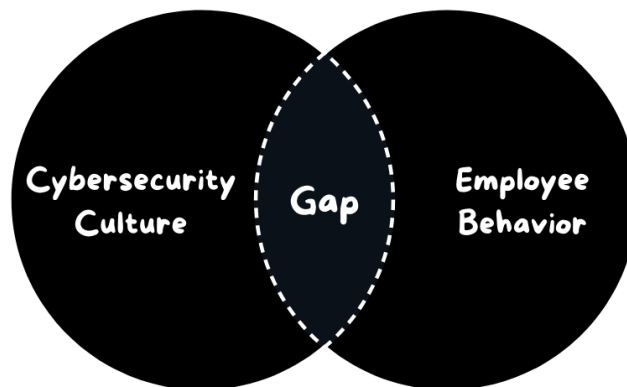


Figure 6: Research Gap

The literatures did not provide much insight into the overall usage of big data tools and technologies, and technology acceptance is considered to be the most

significant predictor of success. From the perspective of the users, acceptance of different features, the product itself, as well as their attitude towards the product can be gained. To gain a better understanding of the acceptance rate of big data technology, it is necessary to conduct a systematic study of the reviews of big data.

This led us to identify several challenges in examining cybersecurity situation awareness. The majority of these challenges should be addressed through collaboration between psychologists, human factors engineers, computer scientists, and cybersecurity experts; however, this multidisciplinary need is itself a challenge.

2.12. Chapter Summary

In light of the above-mentioned researches and other widely conducted studies in the field, it is evident that technology plays a significant role in most aspects of organizations within the business environment, contributing to employee behavior as well as global interactions among subsidiaries, customers and all stakeholders. Even though technology has many benefits and advantages, there are several complications and controversies in the world's business environment.

It is a fact that cybersecurity technology has proven its importance over the past decades, particularly in the governmental sector. A variety of factors can affect and influence user behavior through the use of this technology. Our upcoming chapter examines what technique is most appropriate for studying cybersecurity behavior among users.

In this chapter, we discussed what other researchers have done and modules that are being adopted in cybersecurity. Based on the objectives formulated in chapter one, the author's study framework is built around such studies. Throughout the

second chapter, we explored the definitions and terms used in the literature and prior studies relating to cybersecurity technology, which helped shape the study. Thereafter, the chapter discussed how internal and external factors affect organizations' cybersecurity culture on employee behavior. Next, theories and models used to measure adoption of cybersecurity behavior were explained, followed by a summary of the research framework. In the forthcoming chapter, we will clarify the methods and procedures used in the study.

Chapter Three: Theoretical Framework, Methods, and Procedures

3.1. Introduction

This chapter discusses in detail the methodology for analyzing the research question, research design, population, sample, interview questions, research tools, data collection/procedures, and statistical methods used during data collection. A key objective of this study is to investigate how summarizes the complete theoretical framework of the study, including previous studies, research variables, and its conceptual framework, as well as its hypothesis. Also, it presents the researcher's philosophy, design process, and approaches used in the research. The chapter concludes with a description of the research model, its development, adoption and statistical methods.

The sections in this chapter are as follows:

1. Introduction
2. Theoretical Framework
 - o Previous Studies
 - o Research Variables
 - o Conceptual Framework
 - o Research Hypothesis
3. Research Philosophy

4. Research Design
5. Research Approach
6. Operational & Conceptual Definitions
7. Research Strategy
8. Data Collection Method
9. Sample Selection Method
10. Research Flowchart
11. Research Sample & Interpretation of Interview Questions
12. Interview Questions Development
13. Machine Learning Pipeline
 - o Machine Learning
 - o Support Vector Machines SVM
 - o Python
 - o Example of Machine Learning in Practice
 - o The Deployment & Selection of the Analysis Methodology
14. Ethical Considerations
15. Chapter Summary

3.2. Theoretical Framework

3.2.1. Previous Studies

Previous studies have been conducted to measure Cybersecurity culture effect on employee behavior, and the following are the most pertinent studies to the formulation of the model for this study:

Author(s) Name & Study Year	Subject	Brief Description
(Andeme Bikoro et al., 2018)	Determinants of cyber security use and behavioral intention: Case of the Cameroonian Public Administration	Using a mixed method, this study examined the rationale behind Cameroonian authorities' intention to adopt and implement cyber security measures. This research was conceptualized through two theories: the Unified Theory of Acceptance and Use of Technology and the Health Belief Model.
(Addae et al., 2019)	Exploring User Behavioral Data for Adaptive Cybersecurity	This paper describes an exploratory study (using TAM) of the feasibility of implementing predictive

		analytics of users' behaviors as a possible tool for developing effective user-based cybersecurity models.
(Alazab et al., 2020)	Block chain technology in supply chain management: an empirical study of the factors affecting user adoption/acceptance	The purpose of the research is to identify factors that hinder or facilitate the adoption of block chain in supply chains, in order to obtain an overview of the most important aspects related to block chain adoption in supply chains. Researchers incorporated UTAUT, TTF, and ISS models into their conceptual model, with trust-based adoption and innovation constructs for information technology innovations.
(Alqahtani & Kavakli-Thorne, 2020)	Factors Affecting Acceptance of a Mobile Augmented Reality	This article aims to identify factors that may influence the acceptance

	Application for Cybersecurity Awareness	of a Cybersecurity awareness application designed for end users.
(Alqahtani et al., 2020)	The impact of gamification factor in the acceptance of Cybersecurity Awareness Augmented Reality Game (cybar)	Using AR techniques, researchers have created an Android app called CybAR. Further, the study examined whether gamification features increase cybersecurity awareness among users of the CybAR app. A combination of the extended unified theory of acceptance and usage of technology (UTAUT2) and the gamification factor was used to predict CybAR app usage
(Robles-Gómez et al., 2020)	Emulating and evaluating Virtual Remote Laboratories for Cybersecurity	Based on TAM/UTAUT factors (perceived usefulness, estimated effort, social influence, attitude, ease of access), the study analyzed how it can affect the intention of

		students to use Virtual Remote Laboratories for Cybersecurity.
(Mohd Ariffin et al., 2020)	Acceptance of mobile payments by retailers using UTAUT model	This study was aimed at identifying the factors that contribute to accepting mobile payments by retailers, as well as the relationship between those factors. The UTAUT model was used to identify the factors contributing to acceptance of mobile payments.
(Abdalla et al., 2021)	Factors influencing the adoption of cyber security standards among public listed companies in Malaysia	The study used TAM and DOI models to determine the effects of technological factors, organizational factors, and individual factors on cybersecurity standards adoption.
(Alqahtani & Braun, 2021)	Reviewing influence of UTAUT2 factors on	Several factors have been identified in the study that

	Cyber Security Compliance: A literature review	may be effective in encouraging employees to comply with the security policies of a particular organization, and the UTAUT2 model has been used to explain the adoption of technology and its impact on employees' compliance intentions and behavior.
(Alzighaibi, 2021)	Cybersecurity attacks on academic data and personal information and the mediating role of Education and employment	There are many factors that may influence perceived ease of use of cybersecurity, as well as the influence of perceived ease of use on attitudes towards using cybersecurity, the influence of attitude towards using cybersecurity on actual use of cybersecurity, and the influence of job positions on perceived

		ease of use and attitude towards using cyber security, as well as on actual usage of cyber security
(Branley-Bell et al., 2021)	Developing and Validating a Behavioral Model of Cyber insurance Adoption	Authors of this study identified the key factors influencing cybersecurity decisions. Combining PMT and TPB, the model could guide future cybersecurity interventions
(Kabir & Islam, 2021)	Behavioral intention to adopt block chain technology in Bangladeshi banking companies	As much behavioral theory is available to explain technology adoption in the banking industry, this study attempts to explain the factors driving the adoption of block chain in banking. The extended Technology Acceptance Model (TAM) is used in this study because it has a proven record of

		predicting technology acceptance.
(Ng et al., 2021)	Protecting Against Threats to Information Security: An Attitudinal Ambivalence Perspective	Authors discussed the theoretical and managerial implications of identifying the determinants and outcomes of attitudinal ambivalence in the information security context. This work contributes to the information security literature by incorporating attitudinal ambivalence, which arises from the interpersonal and interpersonal appraisal processes, into PMT. Moreover, this work provides insights into designing effective fear appeals to avoid triggering attitudinal ambivalence and thus

		encouraging adoption of security protection behavior
(Abu Afifa et al., 2022)	Block chain adoption in accounting by an extended UTAUT model: empirical evidence from an emerging economy	An extended Unified Theory of Acceptance and Use of Technology (UTAUT) model was used to investigate whether accountants intend to use block chain from their perspective (in accounting)
(Krishna et al., 2022)	Examining the Relationship between National Cybersecurity Commitment, Culture, and Digital Payment Usage: An Institutional Trust Theory Perspective	Based on the institutional trust theory, researchers discuss the effects of NCSC on digital payments usage (DPU) across nations.
(Younus et al., 2022)	The role of behavioral intentions in implementation of bitcoin digital currency factors in terms of usage and acceptance in New	The study aimed to determine whether social affect and cybersecurity have beneficial effects on bitcoin acceptance. Researchers used the Unified Theory of

	Zealand: Cyber Security and Social Influence	Technology Acceptance and Use (UTAUT) to analyze how social impact affects bitcoin acceptance and usage
(Rashed Mohamed Al Humaid Alneyadi & Kassim Normalini, 2023)	Factors influencing user's intention to adopt user's AI-based cybersecurity systems in the UAE	In this study, factors influencing users' intention to adopt AI-based cybersecurity systems in the UAE are investigated using an extended PMT technique.

Table 2: Researches on Cybersecurity Measurement Models

3.2.2. Research Variables

The purpose of this study is to examine how Cybersecurity culture affects employee behavior in the Bahraini government sector. The variables used for this study are two independent variables, and one dependent variable. Table 2 shows these variables:

Independent Variables	Dependent Variables
External influences	Cybersecurity Behavior
Organizational Mechanisms	

Table 3: Research Variables of the Study

Furthermore, for every independent variable, there are sub factors and they are displayed in the following table:

Independent Variables	#	Sub Factor
External influences	1	Societal Cybersecurity Culture
	2	External Rules and Regulations
	3	Peer Institutions
Organizational Mechanisms	1	Cybersecurity Culture Leadership
	2	Performance Evaluations
	3	Rewards and Punishments
	4	Organizational Learning
	5	Cybersecurity Training
	6	Communications Channel
	7	Budget

Table 4: Sub factors of Independent Variables of the Study

3.2.3. Conceptual Framework

A conceptual framework for the study can be found below:

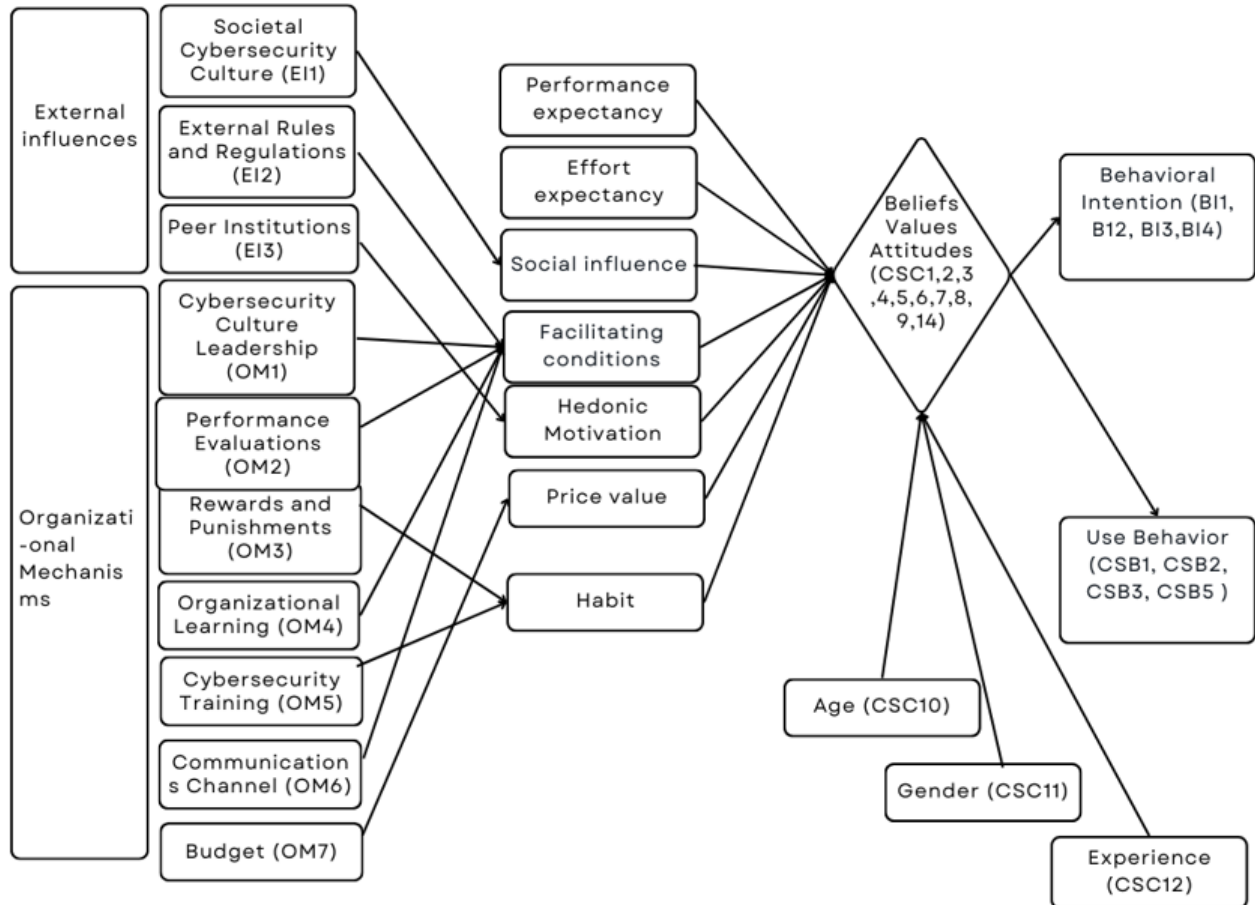


Figure 7: Study Conceptual Framework

The conceptual framework has two independent variables and one dependent variable, as indicated in the above figure. External factors and internal mechanisms make up the independent variables. Whereas cybersecurity This model is centered on cybersecurity culture, which is the dependent variable.

3.2.4. Research Hypothesis

The study was designed to ensure a high degree of precision in its research data by including governmental employees in Bahrain's IT departments of all levels of management and non-management (entry level, junior level, senior level, manager level, executive level, and board of directors' level) . In addition, based on the framework of research acquired from Huang & Pearlson (2019) and further developed by the researcher, the research problems, as well as the objectives of this study, the following hypotheses have been developed to investigate how different factors impact cybersecurity culture in a work environment.

Hypothesis 1

→ H1.0. External Influences do not influence Cybersecurity Culture in Bahrain.

→ H1.1. External Influences Influence Cybersecurity Culture in Bahrain.

Hypothesis 2

→ H2.0. Organizational Mechanisms do not influence Cybersecurity Culture in Bahrain.

→ H2.1. Organizational Mechanisms Influence Cybersecurity Culture in Bahrain.

Hypothesis 3

→ H3.0. cybersecurity culture does not influence Cybersecurity employee behavior.

→ H3.1. cybersecurity culture influence Cybersecurity employee behavior.

3.3. Research Philosophy

In order to ensure flawless research, a researcher's selection of the research philosophy is crucial to be taken into consideration during the design stage of the research. According to Chia (2002), philosophy is concerned with rigorously establishing, regulating and improving the methods of knowledge-creation in all fields of intellectual inquiry, including management science. Among the three main philosophies of research, Bryman (2016) cites positivism, interpretivism, and critical realism.

To select a research philosophy for the current research, it is important to consider all three, and the researcher has the choice of selecting one. For this selection, a definitive definition should be extracted from previous literature and understood clearly. In light of this, below are three research philosophies:

1. Positivism Research Philosophy

A positivist definition, according to Bryman (2016), encompasses the process of gathering data through observation of the causes and effects of variables in order to measure the conclusions of a study objectively. In addition to experiments, questionnaires, and surveys, this philosophy is closely related to quantitative research. Statistics and hypothesis testing are heavily relied upon to reach definitive conclusions. To implement this philosophy, a researcher will need to develop hypotheses, research questionnaires, and distribute surveys to conclude the research with definitive results, based on, as explained earlier, cause-and-effect.

2. Interpretivism Research Philosophy

Bryman (2016) describes interpretivism as relying solely on qualitative data collection methods because knowledge is subjective and context-dependent; thus,

focus groups and interviews are performed. A researcher implementing this philosophy would be required to conduct numerous interviews and focus groups in order to obtain a better understanding of the different perspectives and perceptions of the targeted individuals.

3. Critical Realism Research Philosophy

According to Bhaskar (1978), critical realism is a combination of interpretivism and positivism, suggesting that our social contexts and perspectives are limited by how we perceive our reality, whereas the reality underlying the actual meaning arises from an independent reality independent of our perceptions of it. This philosophy seeks to obtain a complete understanding of the subject matter through the collection of quantitative and qualitative data. The method is highly utilized in a combination of research methods. If the researcher is to implement this philosophy, that would entail gathering qualitative data about the employee's cybersecurity behavior, while quantitative data would be gathered in accordance with the variables associated with cybersecurity culture influences on employee security behavior.

3.4. Research Design

One of the most critical aspects of conducting a study is the design of research. Designing a research study is the process of collecting and analyzing data in accordance with a framework. Research design is perhaps one of the most important decisions a researcher makes after identifying the topic and formulating the research questions. Basically, a research design outlines how a study will go from the research purpose to the outcomes. This process involves the gathering and analyzing of data to improve an individual's understanding of a topic. Research generally consists of three steps: posing a question for examination, collecting data

to answer the question, and presenting an answer to the question (Abutabenjeh & Jaradat, 2018). Research design as explained by Creswell (2014) provides the researcher with a structured plan for conducting research in a highly systematic way and it ensures a flawless result for the study due to providing a reliable and valid methodology. Additionally, the type of research, the sample size, and the methods used in the data collection are included in the research design. Saunders, et al. (2019) contend that a proper research design is paramount to the success of a study, since it enables the objectives and questions to be aligned.

The research design selected for this study must first be defined in order to determine what type of design the researcher will choose. In accordance with this, the following types of research design are listed from a variety of sources:

1. Quantitative Research

The quantitative research design, as described by Creswell (2014), tests hypotheses with numerical and statistical analyses. The deductive approach is used in this type of research, meaning the conclusions come from universal facts to specific conclusions, i.e., from the broad to the specific conclusions. It generally consists of surveys, questionnaires, and experiments conducted in a structured manner.

Research design strategies used in quantitative research include:

Experimental Research	In experimental research, variables are examined and controlled through manipulation. Typically, two variables or more are studied. Data collection takes place in a controlled environment according to Sekaran & Bougie (2016).
-----------------------	---

Quasi Experimental Research	Like experimental research, quasi experimental research has an independent variable without complete control. Researchers compare the results using groups that have already been established (Sekaran & Bougie, 2016).
Causal Comparative Research	The casual-comparative research method involves comparing two groups with one, two, or more variables that are different. It involves the collection of data via observations, questionnaires, or surveys to determine the effect of variables on outcomes. Seekaran & Bougie (2016) describe this approach as a method for examining the influence of variables on outcomes.
Machine Learning	In essence, machine learning is about teaching machines how to make predictions based on data sets A machine learning technique is a set of mathematical models that solve high nonlinearity problems across a wide range of topics: prediction, classification, data association, and data

	conceptualization (Martinez Torres et al., 2019).
--	---

Table 5: Quantitative Research Design Strategies

2. Qualitative Research Design

A qualitative research design involves interviewing, conducting focus groups, and observing for research purposes. Kitto et al. (2008) describe qualitative research as systematically capturing, ordering, describing, and interpreting textual data gathered from interviews, observations, and documentation. Techniques such as interviewing, observing, and analyzing documents are included. This type of design examines individuals and groups in their natural environment in order to understand their behavior, processes of interaction, and values and meanings. In terms of analysis, this type of research design provides a comprehensive overview of participants' perceptions and beliefs. Researchers typically use it in situations that are difficult to quantify.

There are several strategies involved in designing qualitative research, including:

Phenomenology	Philosophically, phenomenology refers to a paradigm, a methodology, and it is associated with qualitative research. The purpose of phenomenology is to understand how people make sense of their experiences (Starks & Brown Trinidad, 2007).
Grounded Theory	It consists of collecting data from participants to form a theory based on that data. Through observation and

	interviews with participants, this type of research can be conducted Charmaz (2014).
Ethnography	Anthropology is centered on observing a collective community or interviewing a community or culture in depth. An ethnographer's goal is to provide deep insight into people's views and actions, as well as the natural environment (e.g., sights, sounds) of the place they inhabit via detailed observations and interviews (Reeves et al., 2008).
Case Study	Case study, as defined by Yin (2018), is a qualitative research method that uses observations, interviews, or document analysis to study a phenomenon in a situation or case in an in-depth manner.
Narrative Research	D. J. & Connelly (2000) stated that narrative research involves listening to participants' stories and narratives and analyzing them to gain a comprehensive understanding of their values and perspectives.

Table 6: Qualitative Research Design Strategies

Selection of Research Design – Quantitative & Qualitative

We adopted methodologies from a wide range of previous literature, notably Huang & Pearlson's research (2019). A model similar to the one proposed in their paper has been selected for conducting the same kind of research on Bahraini government

employees. To achieve a comprehensive overview, the researcher included a few additions, considering today's cybersecurity culture in government.

Current Research Selection:

This study encompasses both quantitative and qualitative methodologies of data analysis. A quantitative method of research is utilized by developing interview questions acquired from previous research, and by making minor additions to survey questions acquired from earlier studies. One-to-one interviews were conducted with the target governmental employees, face-to-face as well as virtually, and the results were analyzed to test the hypothesis. The researcher, on the other hand, used qualitative research to gather information from prior literature on the subject of the study, and then systematically extracted the data from the literature, thereby guiding the development of the research design and implementing the research model that is used in this study. A descriptive research method was chosen by the researcher as part of the quantitative research design, and it was used to analyze the study's results through machine learning, Support Vector Machines (SVM) to the results of the study. Kumar (2015) supports this method and states that it determines the relationship between independent and dependent variables. As well as being an inexpensive method of conducting research, the researcher chose the interview method since it produces clear and precise responses. Aquino, et al. (2018) chose this method because it reaches a specific population sample that is sought after and has minimal communication barriers and misunderstandings since direct one-on-one interaction between interviewer and interviewee enhances communication.

As a whole, and to summarize, both primary and secondary research were conducted for this study. The primary research method involves conducting in-

person and online structured interviews, as well as inputting data into Google Forms.

3.5. Research Approach

In order for the researcher to conduct a successful research study, plans or strategies must always be carefully developed beforehand. Testing hypotheses and answering research questions is highly dependent on systematic data collection, analysis, and interpretation, as noted by Creswell & Creswell (2017). As part of the design of research, guidance should be available so the researcher can knowingly follow procedures and apply techniques.

When it comes to research approach, there are three primary methods a researcher can utilize, and they are the inductive approach, deductive approach, and the abductive approach. As defined by Creswell & Creswell (2017) in their book titled “Research design: Qualitative, quantitative, and mixed methods approach”, the definitions of each are as follows:

The Inductive Approach: Beginning from the specific collection of data to form a universal theory. For example, observing animals acting differently and running away from a specific location brings the observer to the conclusion that a catastrophic event is about to happen soon, like an earthquake, volcanic eruption, or a tsunami.

The Deductive Approach: Opposite to the inductive approach, beginning from the universal theory to reach the specific conclusion. For example, observing a catastrophic event soon to take place may bring the observer to the conclusion that the animals within that specific location will be acting differently and run away from the location.

The Adductive Approach: Is a mixture of the two previous approaches. This approach is usually considered by researchers when there is a lack of information. For example, observing a tire print in a road before a traffic light may bring the observer to the conclusion that a car had previously pressed full brakes at a high speed to stop before a red light, even if the observer had not actually seen the car doing the activity.

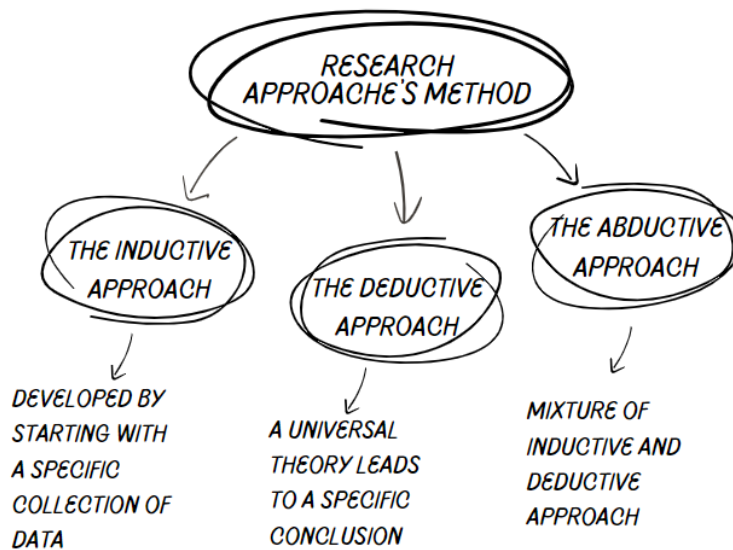


Figure 8: Research Approaches Methods

Current Research Selection: When it comes to the current research, the researcher has selected the deductive approach for the following reasons:

1. It assists the researcher to come to the conclusion from the universal to the specific.
2. It helps the researcher create theoretical constructs (the hypothesis) by deducting from the general perspectives.

3. It generates a meaningful exploration for the development of the theoretical framework
4. It supports the requirement to attain a complete understanding of the specific influencing factors of cybersecurity whether they are positive or negative.
5. It achieves substantial effectiveness and efficiencies when it comes to applying the operational term of the theoretical framework and the hypothesis.

All in all, the deductive approach is accepted in this research as it is in line with the objectives of the research and the empirical analysis intended for achieving high accuracy in data collection, analysis and reaching the conclusion of the study.

3.6. Operational & Conceptual Definitions of Variables

To conduct effective research, it is imperative to have a thorough understanding of each variable's definition before beginning. Thus, the researcher presents the reader with specific literature-supported definitions of the variables.

There are two fundamental classifications of defining variables before moving to the definitions of each variable. They are:

Operational definitions	Conceptual definitions
operational definition according to Shadish, et al. (2002) refers to the methods the research undertakes to measure a variable. It is important to also note that the operational definition is taken from the research design and its	conceptual definition according to Church (2004) refers to the dictionary meaning of the variable. whereas the conceptual definition is defined by the researcher and the definitions are supported by

measurability is quantifiable with no misinterpretation	previous literature, however their measurability is non quantifiable and subject to different interpretations.
---	--

Table 7: Types of Definitions of Variables

A table has been provided below to summarize for the reader the definition of each variable:

Variable Type	Variable	Conceptual Definition	Operational Definition
Independent Variable	External influences	Factors affecting the cybersecurity culture in governmental organizations and their sub factors	A Likert-Scale is used to measure this variable during interviews, 5 points, three questions.
	Organizational Mechanisms	Organizational factors and sub-factors that affect cybersecurity culture.	A Likert-Scale is used to measure this variable during interviews, 5 points, six questions.
Moderating Variable	Cybersecurity Culture	Values, beliefs, and attitudes about cybersecurity	A Likert-Scale is used to measure this variable during

		expressed in an organization	interviews, 5 points, fourteen questions.
Dependent Variable	Behavioral Intention	Employees' intentions resulting from the cybersecurity culture	A Likert-Scale is used to measure this variable during interviews, 5 points, four questions.
	Cybersecurity Behavior	Employee security behavior resulting from cybersecurity culture	A Likert-Scale is used to measure this variable during interviews, 5 points, five questions.

Table 8: Summary of the operational and conceptual definitions of the variables

3.7. Research Strategy

It is imperative that researchers use research strategies that facilitate consistent and reliable analysis in order to attain reliable results. Using a quantitative and deductive approach, the current study examines the effect of cybersecurity culture on employee behavior.

Aside from this, both qualitative and quantitative research can contribute to research in different ways. Basias & Pollalis (2018) note that each has its strengths as well as flaws. They explained that the quantitative method of research is favored since its focus on objectivity ensures that it is reliable. Further, they explain that a hypothesis or theory is better tested using quantitative research methods. On the

other hand, qualitative research methods are more suitable for dealing with complex issues.

Current Research Selection:

The current research relies on quantitative analysis via the analysis of the results of open-ended interview questions as part of a qualitative approach to the study. By using this method, the researcher can reach specific conclusions without being influenced by external influences. It also limits observing while boosting numerical results. All variables of the study are measured through this study's analysis of responses. As a result, the quantitative use of research strategy aids in conducting systematic analysis, producing reliable results, and achieving high efficiency in achieving the objectives of this study.

3.8. Data Collection Method

Research methods that are to be used for the purpose of collecting the data for analysis at a later stage are highly important for a researcher to consider. Two types of data collection methods exist for collecting data: primary and secondary. Primary is the method used to collect direct data, and secondary is the method used to collect indirect data.

A table below illustrates the difference between primary and secondary methods for the reader:

Primary method	Secondary method
----------------	------------------

Surveys, interviews, focus groups, polls, and other similar data gathering methods are the primary methods used to collect data. Data collected in this manner, according to Rhodes, et al. (2014), allows the researcher to strengthen their area of research since they are based on data collected from others who have experienced the phenomenon instantly.	This method involves gathering data from previous literature, books, newspapers, articles, and other similar resources. Researchers can use this method to gather data from previous sources, thereby enhancing their research area with existing information. The collection of data refers to using previous literature, books, newspapers, articles, and other sources that provide data for their research.
--	---

Table 9: Methods of collecting data

Current Research Selection:

It is the goal of this study to focus on both methods of collecting data in order to gain a deeper understanding of what previous literature, books, interviews, and online articles had to say about different aspects of the research topic. In this research, secondary sources have been used to gather data and develop an entire framework for research. However, primary research involves conducting interviews and obtaining respondents' responses without any external intervention.

A questionnaire was distributed to the targeted population of IT management, IT specialists, cyber security job responsibilities and others as part of the quantitative data collection process, while interviews with top management were used to collect qualitative data. Data were collected using the following tools:

- a) Interviews: Interviews were conducted with top executives of the selected governmental organizations in the Kingdom of Bahrain to gather qualitative

data for the study (see Appendix A). In these interviews, participants were interviewed face-to-face in a semi structured manner and personal meetings were conducted to collect the required information about the cybersecurity culture within the Kingdom of Bahrain's governmental sector. Word of mouth and referrals from the interviewees led to the selection of the employees. Therefore, this indicates that the sample used is a random sampling method.

Overall, interview questions consist of Six sections, and a total of 33 questions. The sections of the interview are as follows:

1. Discussion topic, introduction, and guidelines
 2. External Influences
 3. Internal Mechanisms
 4. Cybersecurity culture
 5. Intention Behavior
 6. Cybersecurity Employee Behavior
- b) Questionnaires: Based on a literature review and extensive research, questionnaires were designed. An online questionnaire was distributed to 150 respondents in various banks (see Appendix B). Questions were designed using Likert scales, checkboxes, and open-ended formats to provide a quantitative measure of their effectiveness. A questionnaire was developed to examine the cybersecurity culture in government organizations. An illustration of the questionnaire question for each factor is provided in section three of Appendix B. Data were collected from the respondents using a five-level Likert scale (“Strongly Agree” to “Strongly Disagree”)

It is also important to note that the current research paper would not be as effective and efficient if it were entirely based on secondary data, whereas primary data is typically considered reliable and trustworthy, as it is collected from employees who

are familiar with this technology directly. It is further suggested by (Mantha, et al., 2016) that the primary method is up-to-date, accurate, and provides better control over information gathered from respondents.

A 5-point Likert Scale was used in all questions related to the variables and responses were inputted into a Google Form. In-person and online interviews were conducted. Interviews were conducted virtually using Zoom and Microsoft Team as two different platforms for the virtual conduction of interviews. In contrast, in-person interviews took place at several different locations, including respondents' offices as well as coffee shops. A targeted audience is Bahrainis employed in the governmental sector who work (at the time of conducting the research) or worked in a department affected by cybersecurity. After data had been gathered, the SVM algorithm was used in the machine learning pipeline to make predictions, determine which factors have the most influence and what kind of influence they have, and determine whether there is a correlation between employee security behavior and cybersecurity culture.

The interview technique was used for obtaining primary data and was conducted both in person and online. Secondary data was collected through an 'online research technique'.

3.9. Sample Selection Method

To ensure the success of a study, it is crucial to understand the targeted population and sample size. Moreover, in order for researchers to ensure that their sample represents the targeted people accurately, they must select the correct method of sample selection. According to Roulston & Williams (2017), the sample selection method is the process of selecting individuals who are related to and a vital part of

the investigation. As for the definition of population, David (2019) identifies it as a group of individuals who are taken into account when assessing the outcomes of a study.

The following table summarizes the various methods for selecting a sample from a population:

1	Convenience sampling	As Hussain, et al. (2021) explain it, this method consists of selecting willing and accessible participants to participate in research. Researchers with limited resources and time can benefit from this sample selection method because it is inexpensive and quick. The negative side is that such a selection of sample may cause bias since the electorate may not be representative of the entire population of the study.
2	Stratified sampling	It consists of dividing the targeted population into groups and then selecting a subgroup from each group that represents the entire sample of the study population, as defined by Ragin (2017). The process of selecting samples is extremely time-consuming and resource-intensive
3	Snowball sampling	According to Braun, et al. (2017), this method is defined as the identification of participants who are accurately suitable for the intended research at the initial stage of sample selection, and then the selected sample helps spread the word to others who are also interested in assisting in research but fit the same criteria. The method of sample selection is usually chosen by researchers when they have difficulty reaching their intended

		research population. Like a snowball, this method rolls in a loop until the desired size is reached. In spite of this, this type of sample selection can be biased, since participants may form similar opinions on the subject.
4	Purposive sampling	The method, according to Palinkas, et al. (2015), involves selecting sample members based on a specific characteristic, such as occupation or gender. Researchers who aim to answer a question or hypothesis select this method of sample selection. Variables can be controlled using this method. Although this type of sample selection is viable, there is a possibility that it may be biased as a result of an incorrect representation of the entire population.
5	Random sampling	As Babbie (2017) describes it, this method is based on randomly selecting participants from a population, giving everyone in the population an equal chance to participate in research studies. Research that uses a quantitative research strategy typically applies this sample selection method to limit bias.

Table 10: Sample selection methods for a population

Current Research Selection:

For the present study on cybersecurity culture in banking organizations, the researcher has chosen random sampling to collect data. Several research assistants assisted the researcher in choosing employees who worked in the IT sector or had experience in security and safety to participate in the study. Interviews were

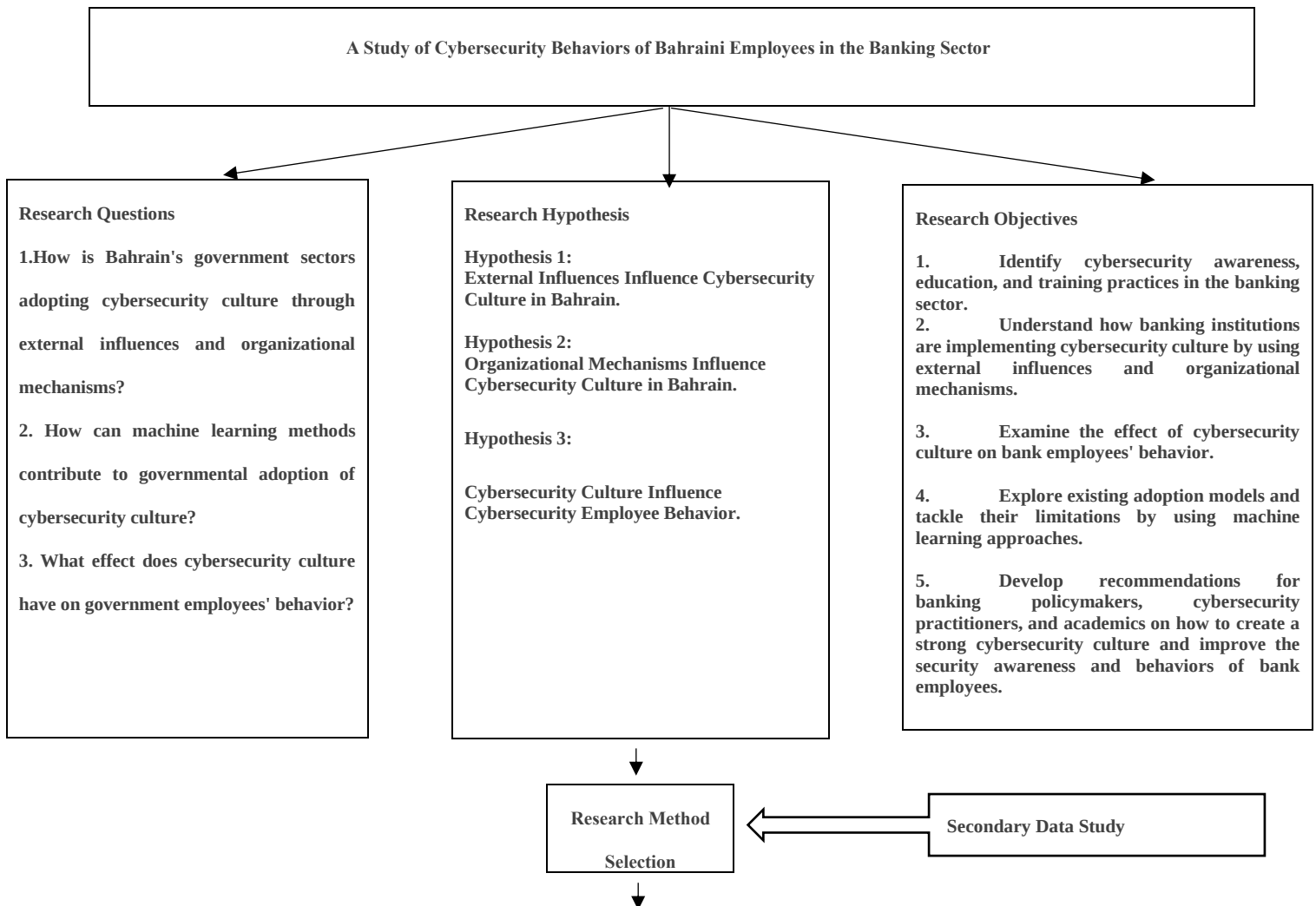
conducted with participants, and once the participants had referred others who might be interested, they were asked to contact those referrals for interviews. Participants are selected according to their fit with the study's context, and referrals are made based on the same criteria. The stratified sampling technique is used, however, when it comes to deploying the acquired data, since the data in the machine learning process is divided into two categories, namely, the training subset and the testing subset. The entire set of data is deployed before this approach is taken. This study is aimed at people in the Kingdom of Bahrain who work in the cybersecurity and information technology sectors or have experience in the security fields, or who are retired, or who have had experience in the security sector. The study's population also includes employees of all levels, from entry-level to senior management, board members to business owners, managers, and executives. Research unit consisted of 100 to 150 randomly selected employees for data collection. All of the workers were treated anonymously and had equal chances of being selected. As opposed to the non-probability sampling technique, which involves the researcher selecting a random sample of participants without involving the researcher's judgement, willingness to participate, or availability, probability sampling is the sampling technique selected by the researcher. Due to the small sample size of the current study compared to the total population of Bahrain's security workers, the researcher selected it. As a sampling technique that provides accuracy, smoothness in handling, precision, and transparency, random sampling is the appropriate sampling technique.

As a whole, 108 participants were recruited for this study, and they were all selected randomly. There was no abandonment of questions for reasons of incomplete or partial answers since the interviewer explained that the interviewee was anonymous in the research which didn't mention any names, positions, or

organizations. Consequently, participants provided complete, unbiased and closed answers to the questions.

3.10. Research Flowchart

According to Creswell & Creswell (2017), the research flowchart represents the entire research visually to the readers and it includes the processes and steps of the study being conducted. It basically provides a complete summary of the research being carried out. Like a map, that guides the reader from start to end and shows the entire destination that is taken.



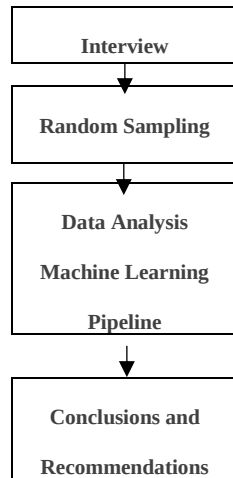


Figure 9: Research Flowchart of the Study

3.11. Research Sample and Interpretation of Interview Questions

A research sample, according to Babbie (2017), is a group of people selected by the researchers for study. The sample represents the entire population, and the conclusions drawn by analyzing the data from that sample represent it as a whole. Because it is usually impossible to study an entire population, researchers select samples from their target populations. It would be almost impossible to study all the IT workers in Bahrain, as there are millions of individuals currently working, or who worked or retired in the IT sector, for the current research examining the effects of cybersecurity culture on employee behavior. As part of assisting in studying the entire population, the researcher could reach out to the government and ask them to distribute the survey via the COVID-19 app on all smartphones in Bahrain, which is downloaded by individuals 18 years old and above. There is the possibility that this method would result in over 300 thousand individuals being sampled and analyzed, making it a time consuming and expensive process. In addition, this research is of great importance to the government, since the

researcher would need to convince government representatives and adjust the research in accordance with government priorities, which may also result in an external intervention, which would negatively affect the study's end result.

As a result, we selected a random sampling technique based on probability. Due to the following reasons, this method has been selected:

1. There is a widespread use of this method among researchers.
2. The bias is limited well by it.
3. All of the population is represented by it.
4. In statistical analysis, there is a minimal margin of error and a high degree of precision.
5. The method is simple to follow.

We conducted 108 interviews, which corresponded to the intended sample size of 100-150. Since the random sampling technique selected 108 responses from the population who held experience in cybersecurity, all 108 responses were used in this study. As part of the interview process, Google Forms is being used to collect data since the researcher is in charge of collecting information, which will then be stacked neatly online for later extraction and cleaning. Using the Machine Learning Pipeline and Support Vector Machines (SVM) algorithm, the responses of the interviewees were analyzed. The participant sample (total 108) provided accurate, complete, and precise data for this study and is acceptable to be included.

Outreach	No.
Interview Invitations	150

Interview Responses	108
Response Rate	72%

Table 11: Response Rate of Interviews in This Study

Outreach	No.	Percent
In-Person Interviews	20	19%
Online Interviews	88	81%
Total	108	100%

Table 12: Type of Interview Conducted in This Study (Online, In-Person)

During the writing of this research paper (and the generation of the documentation of this research paper), Microsoft Word was used, whereas Microsoft Excel (MS Excel) was used to organize the interview questions numerically and consequentially before they were deployed to the final analysis platform. Responses to interview questions were inputted via Google Forms. Data acquired from the interviews were analyzed using Machine Learning, supervised learning technique, the Support Vector Machine (SVM) algorithm is used to predict and make decisions. In addition, each variable was evaluated using a 5-point Likert scale. This study uses the five-point scale so that responses can be measured more precisely. A Likert scale is used because it provides quantitative data that can be analyzed mathematically. The following table illustrates the scores and Likert Scale numbers as well as the intention of the researcher when conducting this study:

Likert Scale 5-Points System	Score
Strongly Disagree	1
Disagree	2
Neutral	3
Agree	4
Strongly agree	5

Table 13: 5-point Likert Scale System

Based on research conducted by Huang & Pearson, (2019), this research framework was created. It provides an overview of certain characteristics of cybersecurity culture elements, including external influences, internal mechanisms, beliefs/values/attitudes and behaviors. As the primary element to apply cyber security to an organization, the researcher has included some elements, including a budget. For the purposes of obtaining an overview of respondents' interpretations of how cybersecurity culture affects employee behavior, the interview questions have been divided into six sections. The following table outlines the sections of the interview and their descriptions:

Interview Section	Description
Section 1: Discussion topic, introduction, and guidelines	Introductions represent introducing the interviewers to the interviewee, discussing the topic of discussion, and outlining the interview's guidelines. These guidelines include: Dear Respondents, We are conducting a field study related to the subject “A study of cybersecurity behavior of Bahraini employee in Banking Sector”. In order to complete this study, the work includes a field survey that has to be filled. The main aim of this survey is you as Information System/ IT manager, those who have cybersecurity job responsibilities and others IT job related employee in your institution to evaluate the factors related to cybersecurity Behavior in organizations, which mainly focus on an investigation in the Bahraini banking sector. It will be greatly appreciated if you participate actively and respond honestly. You can rest assured that All your answers will be treated in the strictest confidence and will be used only for this study. Than You

Section 2: Personal Data	The following section discloses interviewees' personal data, such as their gender, age, marital status, and educational level (university degree).
Section 3: External Influences	A total of three questions are included in this section that measure the external factors that influence cybersecurity culture.
Section 4: Internal Mechanisms	This section consists of seven questions that measure how organizational mechanisms affect cybersecurity culture.
Section 5: Cybersecurity Culture	Cybersecurity culture includes 14 questions that measure the beliefs, values, and attitudes of individuals, groups, and leaders.
Section 6: Behavior Intention	4 questions measure employees' intention to behave in a cybersecurity manner.
Section 7: Cybersecurity Behavior	There are Five questions in this part of the survey that seek to gather information about employees' cybersecurity practices.

Table 14: Interview sections and descriptions

3.12. Interview Questions Development

This study's interview questions are based on the deep case study in (Huang & Pearlson, 2019) research paper. They address the following factors that drive a cybersecurity culture, namely an external influence and internal mechanisms.

Along with the elements they proposed, all of the variables that they deployed in their study have been used in the current study.

The Table below illustrates some examples of cybersecurity culture elements that Huang and Pearlson conducted (Huang & Pearlson, 2019).

Cybersecurity Culture			Example from Case Study
Beliefs, Values and Attitudes	Leadership	Top Management Priority	Executives at Liberty Mutual made cybersecurity a strategic-level priority. For example, they authorized a significant budget for security activities, tools and professionals
		Top Management Participation	A set of regular blog posts on cybersecurity topics from the CISO or his team were mapped out for the year. The CISO himself was often considered the "face" of the campaign
		Top Management Knowledge	Top management regularly engaged in discussions about cybersecurity issues both as part of their leadership team meeting and individually with cyber experts in the company to keep their knowledge current.
	Group	Community Norms and Belief	Slogans such as the "Responsible Defender TM " and "Our Information. Our Responsibility" were part of the everyday conversation.
		Team Work Perception	Employees would regularly compare notes on phishing exercises and discuss other cyber topics.
		Inter-department Collaboration	The core team working with cybersecurity leaders included members from across the enterprise, not just the tech departments
	Individual	Employee's Self-efficacy	Employees indicated that they knew what to do when they received a suspicious email, and knew who to contact should they notice any other potential cyber incident brewing.
		Cybersecurity Policy Awareness	Marketing-like campaigns regularly shared cybersecurity policies and employees indicated they knew what these policies were.
		General Cyber Threat Awareness	Employees were regularly told about cyber threats and were encouraged to take steps to both protect the company asset and their own personal assets.

Behaviors	In-Role Cybersecurity Behaviors		Phishing exercises and subsequent surveys indicated a trend towards stronger security behaviors of all employees.
	Extra-Role Cybersecurity Behaviors		Some employees volunteered to be cybersecurity "first responders" to alert others of suspicious emails or other activity.
Organizational Mechanism	Leadership	Cybersecurity Culture Leadership	The CISO added a role to his team for Cybersecurity Awareness and charged her with building a culture of data protection.
	Incentive	Performance Evaluations	Individuals who repeatedly failed phishing exercises were subject to notations in their performance evaluations and repeated offences could result in poor scores in performance reviews.
		Rewards and Punishments	Failed phishing exercises would result in retraining. Employees who got involved in cyber-related activities were praised and given 'status' in the organization.
	Process	Organizational Learning	The entire organization was continually updated on cybersecurity news and issues through campaigns designed to facilitate long-term retention of cybersecurity practices and behaviors.
		Cybersecurity Training	In addition to employee onboarding, where cybersecurity training was included in new-hire procedures and processes, micro-campaign programs were created to increase awareness. Cybersecurity awareness month made the issue a corporate focus for that period. The team strove to create training that was "engaging and not pedantic."
		Communications Channel	Messaging was a big part of management activities to encourage cybersecure behaviors. The team created a brand and used traditional marketing techniques to spread the message through the company. They used multiple channels including videos, digital displays, blogs, alerts, emails, post cards, events, and training.

External Influences	Societal Cybersecurity Culture		The corporation was part of the financial services industry which, by its nature of managing client information, created a need and set of values and beliefs about how important it was to protect data. Execs reflected this in their prioritization of building a culture of data protection.
	External Rules and Regulations		The organization of the highly regulated industry. For example, regulations and policies like the New York Department of Financial Services Cybersecurity Regulation provide specific and prescriptive requirements.
	Peer Influence		Executives made it clear that their company reputation was dependent on the trust they received from customers, clients, and in general. They articulated that the industry as a whole had to have a high standard for protecting information assets.

Table 15: Case Study Examples of Cybersecurity Culture Elements (Huang & Pearlson, 2019)

Overall, the researcher has the opportunity to base the current study on strong elements of precision, consistency, and objectivity since he has a foundation for the development of interview questions for the current study about cybersecurity culture and its impact on employee behavior.

Due to the importance of this sub factor (Budget), the researcher has added it to the internal mechanisms and also added questions to the interview in order to better understand this study; the researcher believes that this sub factor has a significant impact on the cyber culture, which will be discussed in the results section.

The study of cybersecurity culture can be further enriched by incorporating additional factors that depend on the circumstances in which the study is conducted and whether the added factor has a large impact on the cyber culture in that sector.

As a result of the research, it is important to note that each factor has several sub factors that collectively assist the researcher in reaching a solid conclusion about their effects on employee security behavior. The following table illustrates the factors and sub factors that were explored in the focus group interviews conducted for this research:

Factors / Constructs	Sub factors / Code	Parameters
External Influences (EI)	EI1 – Societal Cybersecurity Culture EI2 – External Rules and Regulations EI3 – Peer Institutions	3 Parameters

Internal Mechanisms (OM)	OM1 – Cybersecurity Culture Leadership OM2 – Performance Evaluations OM 3 – Rewards and Punishments OM 4 – Organizational Learning OM 5 – Cybersecurity Training OM 6 – Communications Channel OM 7- Cybersecurity Budget	7 Parameters
Cybersecurity Culture Factors (CSC)	Group Level CSC1 – Inter-department Collaboration CSC2 – Community Norms and Beliefs CSC9- Teamwork Perception Leadership Level CSC3&7– Top Management’s Priorities CSC4,5&8- Top Management’s Participation CSC6- Top Management’s knowledge Individual Level CSC10&11- General Cyber Threat Awareness	14 Parameters

	CSC12- Employee's Self-Efficacy CSC13&14- Cybersecurity Policy Awareness	
Behavior Intention (BI)	BI1 – Cybersecurity Training and Intention BI2 – Cybersecurity Policy and Intention BI3– External Cybersecurity BI4 – Cybersecurity culture and intention	4 Parameters
Cybersecurity Behavior (CSB)	CSB1 – Cybersecurity Training and Behavior CSB2 – Awareness programs and cybersecurity behavior CSB3–Cybersecurity awareness, training, and education CSB4 – Cybersecurity behavior and Facilitating Conditions	4 Parameters

Table 16: Factors and Sub factors of the Interview Questions of this Study

Finally, according to Rubin & Rubin (2020) it is important to note that using the interview as a form to acquire data provides the research with many benefits including:

1. Exploration of answers in an in-depth manner.
2. Provision of flexibility.
3. Empowerment of participants to accurately share their perspectives.
4. Access to diverse perspectives.
5. It is a practical method for the acquisition of data.
6. Simple for interpretation, visualization, and analyses.
7. Covers all types of topics required for research.

3.13. Machine Learning Pipeline

3.13.1. Machine Learning

3.13.1.1. Introduction

To find out if cybersecurity culture in the government sector impacts employee security behavior, the researcher will deploy a machine learning pipeline. In order to understand this research, the reader must first understand machine learning. Mitchell (1997) wrote a book on machine learning, which gives a complete definition of machine learning in a simple manner.

As a definition, machine learning can be defined as “the study of algorithms that can learn from data and predict or make decisions based on that data. To put it simple, a computer learns from data and improves its performance on specific tasks by designing algorithms and statistical models. Using advanced computer technologies (artificial intelligence), it makes predictions and decisions without explicit programming by learning from data.

3.13.1.2. Machine Learning Steps

In order to deploy its powerful outcomes, machine learning follows a specific pipeline. In the following figure, each step of the machine learning pipeline is

presented in brief and followed by a table containing specific details about each step:

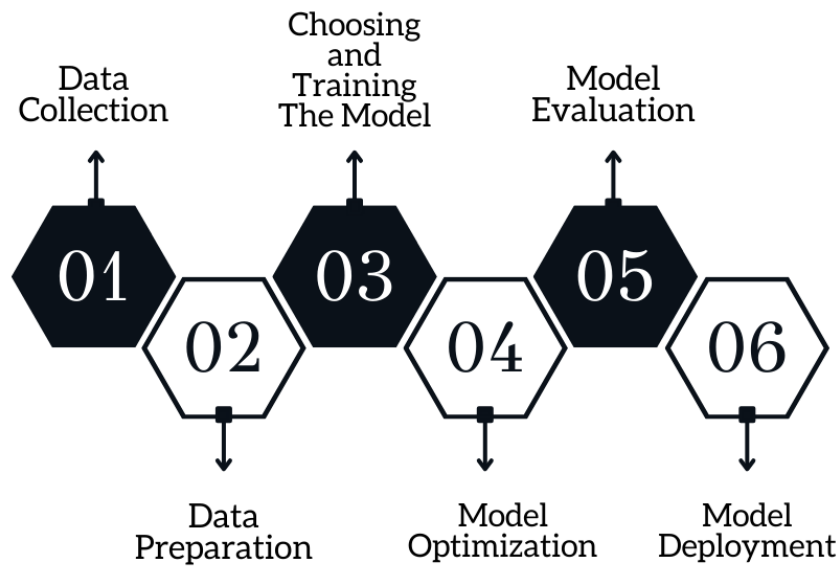


Figure 10: Machine Learning Steps

Figure13 illustrates the pipeline of machine learning steps from data preparation to model training, model optimization, model evaluation and deployment.

Here are the detailed steps of the machine learning pipeline as gathered from a variety of sources:

Step	Details	Reference
Step 1	Various sources of data are collected, such as databases, application programming interfaces (API) and files.	Kumar & Kim (2017)

Collection of Data		
Step 2 Preparation of Data	Through the cleaning, preprocessing, and transformation of the data, the data is prepared to be used for machine learning.	Zhang, et al. (2019)
Step 3 Feature Engineering	To ensure that the model is reliable, one of the most important steps in machine learning is selecting the most important datasets and variables.	Li, et al. (2018)
Step 4 Selection of Model	The choice of a machine learning algorithm is determined by the type and amount of data available to solve the problem.	Abu-Mostafa, et al. (2012)
Step 5 Training the Model	By training the model on the data, it is able to learn and identify patterns and relationships between the data.	Goodfellow, et al. (2016)
Step 6 Model Evaluation	Several aspects of the model are evaluated to measure its performance and identify improvements that can be made.	Dietterich (1998)
Step 7 Hyper parameter	The settings of the behavior of the machine learning algorithms are tuned to improve the model performance.	Bergstra & Bengio (2012)

Step 8 Model Deployment	By evaluating new data sets, a trained model can make predictions or make decisions based on them	Breiman (2001)
-------------------------------	---	----------------

Table 17: The steps of machine learning

3.13.1.3. Machine Learning Techniques

Machine learning uses a variety of learning techniques, and each has pros and cons. Machine learning uses a variety of learning techniques that can be used in different ways. A brief description of each technique is presented in the following table:

Machine Learning Techniques	Brief Description
Supervised Learning	The machine learns by analyzing data, labeling it, and predicting new, unseen data.
Unsupervised Learning	By learning from unlabeled data, the machine identifies structures and patterns
Semi-Supervised Learning	The machine learns based on labeled data and unlabeled data.
Reinforcement Learning	Learning occurs when an algorithm receives feedback in the form of rewards or penalties while working in a specific environment
Deep Learning	Machine learning is based on artificial networks that are structured in multiple layers, modeled

	based on the human brain for the purpose of understanding complex data representations.
Transfer Learning	Learning occurs when a machine is trained on a task and then is implemented on another similar task
Ensemble Learning	The machine learns by applying different methods of learning in order to reach the best prediction possible

Table 18: Description of Machine Learning Technique

3.13.1.4. Learning Techniques Illustration

There are three types of machine learning techniques illustrated in the following figure: supervised, unsupervised, and reinforcement learning. In each of the learning techniques, there are algorithms

that are used; those listed are the most popular algorithms according to Jovel & Greiner (2021).

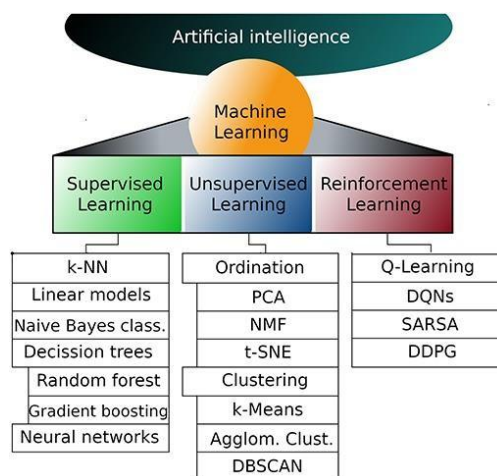


Figure 11: Illustration of Machine Learning Techniques

According to the previous figure, machine learning is a branch of artificial intelligence that acquires experience from calculating algorithms, since when it learns enough it can predict outcomes. To emphasize the supervised learning section of the previous graph, it adopts the decision tree and random forest algorithms, as the learning techniques for machine learning, in this study on cybersecurity culture influences and employee behavior.

3.13.1.5. Supervised Learning

Among the most popular machine learning techniques, supervised learning deals with classification and regression, according to Jovel & Greiner (2021).

It is important to understand that the supervised learning technique deals with labels, for example, the dataset is first labeled according to categories such as (in this case) the external factors, internal mechanisms, etc. The second set of data is characterized by a numerical variable, for instance, employee perceptions about how cybersecurity culture is influenced by external factors. After the data is classified, it is used to train the model with a subset of 60 to 75% of the data, and once the model is trained, a test subset of data is used for prediction and decision making.

3.13.2. Support Vector Machines SVM

SVMs have shown remarkable success in a variety of real-world applications and are among the most popular ML algorithms. BOSER, GUIRON, and VAPKIN introduced the Support Vector Machine (SVM) for the first time in 1992, at COLT 92.

The support vector machine (SVM) is a machine learning technique based on binary linear classification (Boser et al. 1992; Cortes and Vapnik 1995). It separates classes based on the largest gap between the border line instances (called Support Vectors), hence it is known as an optimal margin classifier (Chauhan et al., 2018).

A Support Vector Machine (SVM) is a machine learning tool used for classification and regression prediction that maximizes predictive accuracy while automatically avoiding overfitting. Typically, Support Vector Machines are designed to be able to learn with a learning algorithm derived from optimization theory that incorporates a statistical learning bias, using the hypothesis space of linear functions in a high dimensional feature space. In the NIPS community, support vector machines were initially popular, but today they are an active part of machine learning research all over the world.

Its aim is to find the optimal separation hyperplane so that the margin of the training data is maximized while complexity and overfitting risks are minimized. In addition, once the optimal classification hyperplane has been constructed, an SVM takes very little time to perform the classification process (Ghanem et al., 2017).

SVMs are binary linear classifiers that have been extended to nonlinear data with kernels. SVMs are also classified based on optimal margins. A variety of techniques have been used to model multi-class data, including one-versus-one, one-versus-rest, Crammer Singer, Weston Watkins, and directed acyclic graph models (DAGSVM). There are two types of SVM: linear and non-linear. Linear SVM is suitable for high-dimensional data applications, such as document classification, word sense disambiguation, drug design, etc. (Chauhan et al., 2018).

The SVM model is a powerful supervised machine learning model for classification and regression problems, but it is usually used for classification. The SVM

technique uses hyperplanes or lines to separate classes within a data set in order to classify data (Avci & Koca, 2023).

A linear SVM performs very well in high-dimensional data applications. While their accuracy on test sets is close to that of non-linear SVMs, they are much faster to train for these applications. A document classification application, for example, has a large dimensional input space, and adding features doesn't make much difference since it doesn't make much difference in performance (Chauhan et al., 2018).

Why SVM? SVM is relatively easy to train, and is effective when used with supervised or unsupervised learning applications.

Modeling data with support vector machines is one of the best approaches; they combine dimensionality control and generalization control through generalization control.

SVMs can help improve cybersecurity culture among employees in the area of cyber-security.

$$K(x_1, x_2) = \phi(x_1)^T \phi(x_2)$$

3.13.7. Python

In terms of machine learning languages, there are several that are machine agnostic, and Kumar & Kim (2017) list a few that are most popular, starting with the easiest to use.:

1. Python
2. R
3. Java
4. C++

5. Julia

Currently, the Python language is being used to study the effect of cybersecurity culture on employee behavior for a number of reasons.:

1. Simplicity
2. Flexibility
3. Data analysis, visualization, and modeling libraries and frameworks available

Furthermore, (KDnuggets, 2021) highlighted results of a survey they conducted in 2019, asking the question "What have you used for real-world applications from Data Science and Machine Learning in the past 12 months?". According to 77% of respondents, Python was the most popular language for machine learning, followed by R by 31%.

3.13.8. Example of Machine Learning in Practice

In order to further clarify the process, the following example illustrates how the machine learning pipeline has been utilized to identify the best parameters in a study conducted by Omar, et al., (2023):

Machine Learning Pipeline	How it was done	Results
1. Dataset Collection	Using a questionnaire	A survey was conducted among 150 respondents
2. Data Preparation	An analysis-compatible format	An algorithmic learning model can be

	has been developed by cleaning, preprocessing, and transforming the data extracted from the questionnaire	built based on the survey data
3. Feature Engineering	Choosing relevant datasets to be used in the model.	There are no missing values or outliers in the dataset, and some correlation can be found between the independent variables
4. Selection of Model	Using supervised learning and Support Vector Machines (SVM).	As a popular model, Support Vector Machines (SVMs) are selected
5. Training the Model	It is based on the SVM algorithm.	Training and testing datasets were created.
6. Model Evaluation	Several SVM models are examined and the least impure model is selected for the research.	Selecting the final model

7. Hyper parameters	Python is used at this point to program the model, and all algorithms are further tuned at this point to improve its performance.	A prediction and decision-making model are ready for receiving the entire dataset.
8. Deployment	Predictions are automated using Python and SVM	IA member size, management support, and digital transformation all have a strong relationship with internal audit effectiveness

Table 19: Practical Applications of Machine Learning

3.13.9. The Deployment & Selection of the Analysis Methodology

Accordingly, the following section summarizes the research analysis approach used in the current study on the effect of cybersecurity culture on employee behavior.

In this study, computer learning is used to make predictions and decisions based on data input. Machine learning follows a pipeline that consists of a series of steps that assist computers in making accurate predictions and decisions.

The SVM algorithm is used for regression and classification in supervised learning. A support vector machine learning algorithm is intended to find optimal solutions when the number of training data is limited and large numbers statistics cannot guarantee the optimal solution (Mustafa Abdullah & Mohsin Abdulazeez, 2021).

Using Support Vector Machine (SVM), this study uses the tool for maximizing predictive accuracy while automatically avoiding overfitting to data due to its good results when used for learning applications. The Support Vector Machine has been shown to be successful when used for pattern classification problems. The Support Vector Machine is applied to a particular practical problem by answering questions related to the problem definition and the design of the problem. As a classification technique, SVM is relatively easy to train, scales relatively well to large data sets, and allows users to explicitly control the trade-off between classifier complexity and error

Python is used throughout the data analysis of this study because it is the most popular coding language at the time of conducting this research, and it is also simple to learn and use.

Proposed Model (Equation)

Using the machine learning pipeline, the interview questions are converted into a dataset that includes all the variables and their values. As part of the analysis, the first step is devoted to descriptive analysis (looking at the shape and structure of the data, analyzing missing values, and analyzing descriptive statistics), whereas the second step involves model development, which is geared toward achieving a mathematical relationship between all variables and the outcome.

External Influences = (X1) = Organizational Mechanisms (X1) Cybersecurity Culture= (X2&3) Behavior Intention = (X3)

Cybersecurity Behavior is the outcome.

Inputs X1, X2, X3 are as follows:

- X1 is External Influences and Organizational Mechanisms
- X2 is Cybersecurity Culture
- X3 is Cybersecurity Culture and Behavior Intention

A further point to note is that each factor is made up of several sub factors, and in order to simplify the equation, the researcher purposefully avoided adding all the sub factors within it.

Since the SVC Classifier is used in the current study on cybersecurity culture's effects on employee behavior, the model chosen here is not based on rules. This means that the proposed equation cannot be used in this research for the same reason as previously mentioned, but it may be used in other rule-based models and by researchers in their studies in other fields.

3.14. Ethical Considerations

Research papers must reflect an ethical sense of conduct from the beginning, as the definition of ethics in research differs from traditional ethical standards, but both ultimately originate in the same place. Researchers must act ethically, and ensure that data collected will be accurate and accurate, especially when it comes to data collection based on authentic and real information, according to Miller, et al. (2015). It is therefore necessary for a researcher to set up ethical data collection rules and to follow those rules in order to maintain a flow of information in the field of research and to advance knowledge, as well as to prevent factual falsification, which creates uncertainty in the field, and which may cause turbulence in the flow of data in the general sense and result in misinterpretations of knowledge. As a Basically, research is a collaborative endeavor among

researchers based on mutual respect and trust, ethical principles aimed at the benefit of society and the world, as defined by Saunders, et al. (2015). Public knowledge should be shared in a truthful manner, especially when the work presented is accounted for by the public, making the researcher accountable. Hannes & Parylo (2014) also argue that during the research process, the primary source of data for a study must be data obtained from a sample of the targeted population, and public participation in research is essential for the provision of highly accurate, robust data. The prevention of plagiarism is equally important wherever ethical considerations are involved in research. In addition to reducing fraud, when a researcher adheres to their moral standards in their research, the number of fraudulent activities is minimized; however, when a researcher provides fraudulent data, they cause chaos and can have a drastic impact on society. Furthermore, ethical considerations in research are regarded as guiding principles for social and moral values, promoting honesty, positive behavior, and eliminating data manipulation. Last but not least, Rothstein, et al. (2020) claim integrity, consistency, and respect for intellectual property are all important aspects of research ethics, and they should be considered as part of ethical considerations. While the researcher should take extreme care when it comes to collecting, entering, analyzing, and reporting data, it is essential that the researcher ensures accuracy and correctness of the data collected, input, and reporting.

3.15. Chapter Summary

As a result of chapter three, this study's entire framework was provided. The study was described in detail, the model adopted was explained, a flowchart was provided to illustrate the research, and methods for collecting the data were explained, as well as the use of qualitative and quantitative approaches

to authenticate the impact of cybersecurity culture on employee behavior in the public sector. The chapter also sheds light on the population selected for the research as well as the data collection methodologies, also discusses the conceptual and operational definitions of the variables, and explains in detail how the interview questions that are used in the current study were developed. The implications of cybersecurity culture on employee behavior are also discussed in this chapter, using machine learning as a tool. Based on the research conducted, various techniques for machine learning in the workplace are used, including supervised and unsupervised learning. Therefore, the researcher has decided that the most appropriate machine learning technique for this study is the supervised learning technique. We propose a model for how cybersecurity culture affects employee behavior based on machine learning by deploying a machine learning pipeline. Using the developed model, any user can predict employee behavior based on the variables used herein, which are external influences and internal mechanisms that affect cybersecurity culture. As a result of the interview questions, labeled data can be obtained from a sample of the population, which are the variables and the known outputs. As a result of the collected data, a supervised learning approach is used to determine outcomes based on the known variables, and thus obtaining the final outcomes from a SVM learning approach, based on a combination of the predictions from various decision trees and the prediction and decision making from the randomly created decision trees. Basically, supervised learning uses variables with known outcomes, so to sum up, the machine learning pipeline extracts the results of interviews into a dataset that includes all variables, their values, and the outcomes of those interviews. A descriptive analysis is the first step in the analysis process (between analyzing

data shape, analyzing missing values, analyzing descriptive statistics, and visualizing data). During the second step, the model is designed to achieve a mathematical relationship between all the variables and the outcome.

The following chapter will bring together all the sub-outputs obtained throughout the study, as well as the key results of the analysis stage, and explain the fundamental results in depth.

Chapter Four: Data Analysis, Results, and Discussions

4.1. Introduction

This chapter presents the interview findings, profiles of interviewees, and an analysis of the machine learning pipeline implemented by the study's participants. This chapter illustrates the results with graphs based on the data acquired from interviewees' responses, walking the reader through the pipeline from input to output of machine learning.

In the pipeline of this chapter, the graphs and data results are explained, and the chapter concludes with the results of the study. Overall, the hypothesis is either accepted or rejected at the end of this chapter.

In this chapter, we will discuss the following sections:

1. Introduction
2. Interview Findings
 - Data Editing
 - and Coding
 - Data Entry
 - Interviews
 - Pre-Testing
 - Reliability analysis (Pilot Testing)
 - Preparing and Cleaning the Data
 - General Questions
 - Interviewee Profile
 - Independent and Dependent Variable Questions

- 3. Analysis ○ Dataset Collection ○
 - Data Preparation ○ Feature Engineering
 - Correlation
 - Mean and Standard Deviation ○ Selection of Model ○
 - Training the Model ○ Model Evaluation ○ Results and Discussion
 - Parameters Importance
 - External Influences
 - Internal Mechanisms
 - Overall Factors Importance Measure
 - SVM ○ Research Hypothesis Testing ○ Preview of Research Study Results ○ Chapter Summary

4.2. Interview Findings

The following sections discuss interviews in detail, focusing on the following:

- Data Editing and Coding
- Data Entry
- Interviews Pre-Testing
- Reliability Analysis (Pilot Testing)
- Preparing and Cleaning the Data
- General Questions
- Interviewee Profile
- Independent and Dependent Variable Questions

4.2.1. Data Editing and Coding

Initially, the researcher reviewed the data collected from the interviews to ensure that no values were missing and that the answers of the participants were entered correctly. In order to facilitate the deployment of an organized methodology for entering data by the researcher, a Google Forms online platform was used during the development of interview questions.

The following table illustrates how all questions were coded according to their factors, sub factors, and parameters:

Coding	Type
EI,OM,CSC,BI,CSB	Represents Factor
EI1,OM1,CSC1,BI1,CSB1	Represents Sub factor

Table 20: Coding explanations for interview questions

The following table illustrates the five-point Likert scale used to answer interview questions:

Likert Scale 5-Points System	Score
Strongly Disagree	1
Disagree	2
Neutral	3
Agree	4
Strongly agree	5

Table 21: Likert scale with 5 points

4.2.2. Data Entry

The interviewers inputted the respondents' responses in the Google Forms platform using their mobile phones, iPads, laptops, and computers while they conducted the interviews. Afterward, Google Forms data is converted to Excel Sheets, and the researcher reviews the data in detail to ensure there were no errors during data transfer, as well as to make sure the interviewers' inputs were correct. The data is reviewed and cleaned, then imported into the Python Program Anaconda. The methodology of the machine learning pipeline includes dataset collection and data preparation, all of which are part of the machine learning pipeline.

Additionally, the support vector machine algorithm aids in identifying relationships between variables by categorizing data and testing parameters based on the machine learning pipeline. As soon as the data is input, the machine learns from the learning algorithms it uses to set the model's behavior and provides predictions. This is an easy way to model data, and after the machine learns how to predict datasets, any set of data can be input to it, and the results will be precise and accurate.

4.2.3. Interviews Pre-Testing

The importance of testing the soundness of the interview process and the interview questions is one of the most crucial steps in research before the actual deployment of the interviews. As part of this step, the interview questions and responses are verified to ensure that the questions and responses are reliable, which is important for the analysis phase. It is also vital to ensure that the questions are understood by the recipients and that miscommunication is kept to a minimum.

As part of this research, the interview questions were derived from Huang & Pearson's (2019) previous research study, and they conducted a detailed case study

of one financial services company; the data for the case study were collected over the course of six months through structured interviews.

A similar approach was adopted in preparing and improving the adopted questions in the current research on the effect of cyber security culture on employee behavior. Using Huang & Pearson's (2019) case study elements for guidance. For the purpose of better understanding this study, the researcher has included the sub factor (Budget) in the internal mechanisms as well as added questions to the interviews. It is believed by the researcher that this sub factor plays a significant role in cyber culture. No adjustments were made to the remaining factors or questions.

As part of the testing process, the questions developed and adjusted were added to the Google Forms Online Platform, the interview agenda was developed, and then the interview took place. As a part of the interview testing, a focused group of five employees who worked in the IT sector in a Bahraini banking sector was selected.

We adjusted the interview questions and schedule after conducting the testing, and we reduced the interview time after receiving feedback from the testing sample. In order to provide feedback during the entire interview process, the testing sample was asked to focus on the interview questions, process, and agenda. Their comments focused primarily on how long it took to conduct the interview, and the questions in the newly developed sections. In regards to the sections of questions adopted from the previous research; no negative feedback was received.

After the interview was adjusted, it was conducted with a sample of 10 employees from different banking sectors in Bahrain (each team member was responsible for receiving feedback from two samples). Despite negative feedback from the new test sample, the interview process was found to be reliable and valid.

4.2.4. Reliability analysis (Pilot Testing)

The reliability analysis, according to Mazz et al. (2006), aims at identifying any errors that occurred during the research process of a study. A reliability analysis is, according to Wriht & So (2018), a type of experiment that allows the researcher to make an assessment of their research before embarking on the full administration of the study; this is usually done on a small group of individuals. A total of 108 people participated in the testing phase of this study.

4.2.5. Preparing and Cleaning the Data

In order to ensure that the data acquired from interviews is correctly entered into the data input system by the interviewing team, the researcher is required to review it, clean it of repetition and bias, and double check it. The researcher must also remove outliers from the data before moving on to the analysis phase. A total of 108 participants were enrolled in the study after the data was fully reviewed. This was due to the researcher's adjustments to the control settings of the interviews, as well as the use of Google Forms and coding to organize data input. In this way, the participants experienced a smooth interviewing process, gained full understanding of the meanings of the interview questions, and the researcher was able to achieve, 100% responses as a result.

4.2.6. General Question

As described in the theoretical framework section of this study, interview questions were developed by the researchers of this study to evaluate the hypothesized model described in the theoretical framework section. An analysis of the external influences and internal mechanisms factors influencing cybersecurity culture is conducted in the interview questions to measure the effect of cybersecurity on employee behavior.

4.2.7. Interviewee Profile

A participant's personal profile, including information on their age, gender, marital status, and educational background, is presented in this section.

It's important to note that the participants are all workers with different job positions who are working in the cyber security and information technology sector, or used to work in any security field related to the banking sector in Bahrain.

Detailed information can be found below:

	Frequency	Percentage
Male	62	57.4%
Female	46	42.6%
Total	108	100%

Table 22: Results of the interview - Gender

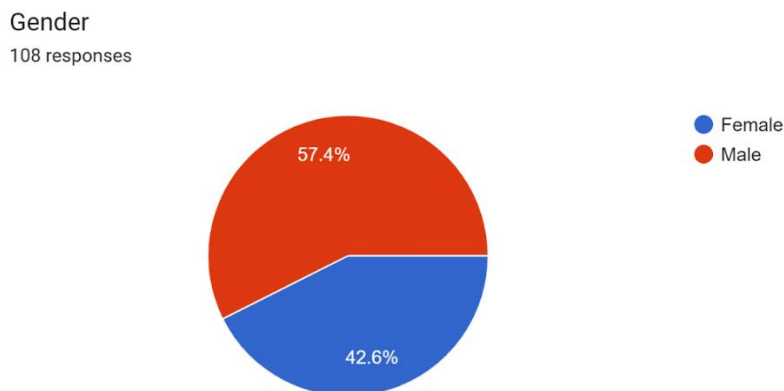


Figure 12: Interview Result – Gender

As shown in the previous table and figure, males and females were interviewed at a frequency and percentage of each. Among the participants of the study, men make

up 57.4% of the sample, while females comprise 42.6%, totaling 108 individuals in total. Females account for 46, while males account for 62, a total of 108 in total. By analyzing the above percentages, we can conclude that more men work in cybersecurity and security sectors than women

4.2.7.2. Age

	Frequency	Percentage
Below 30	42	38.9%
30 to 39 years	59	54.6%
40 to 49 years	5	4.6%
50 to 59 years	1	0.9%
60 and above	1	0.9%
Total	108	100%

Table 23: Results of the interview – Age

Age
108 responses

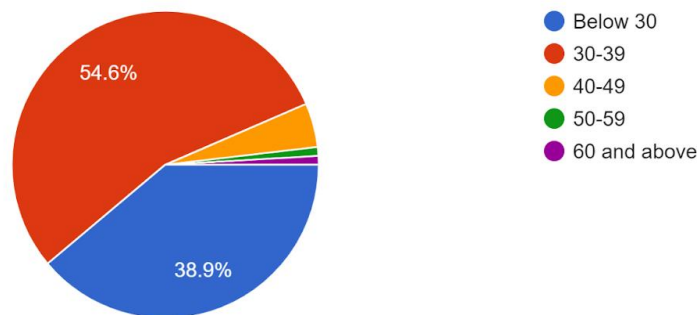


Figure 13: Interview Result – Age

As shown in the above table and figure, 54.6% of participants were between the ages of 30 and 39. The second largest group of participants is those below 30 at

38.9%; the fourth and fifth groups are even at 0.9% each for those 50-59 years old and 60+ years old.

4.2.7.3. Marital Status

	Frequency	Percentage
Single	40	37%
Married with children	54	50%
Married no children	14	13%
Other	0	0%
Total	108	100%

Table 24: Results of the interview – Marital Status

Marital Status
108 responses

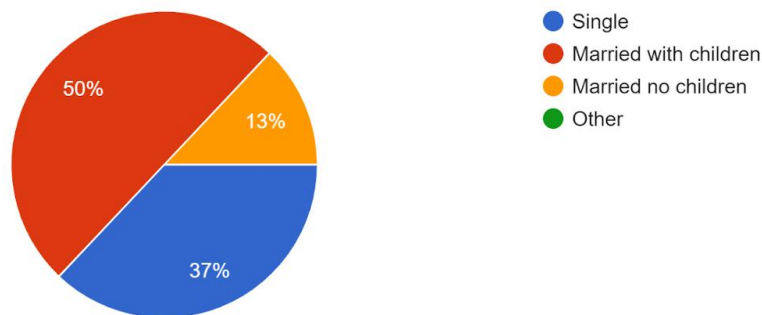


Figure 14: Interview Result – Marital Status

As a consequence of the previous table and figure related to marital status, we can see that most participants in this study are married with children, making up 50% of the respondents; on the other hand, 37% of respondents are single, 13% are married without children, and no other marital status was observed.

4.2.7.4. Education Level: University Degree

	Frequency	Percentage
BSc.	96	88.9%
MSc.	6	5.6%
PhD.	0	0%
Other: Specify	6	5.6%
Total	108	100%

Table 25: Interview Result – Education Level

108 responses

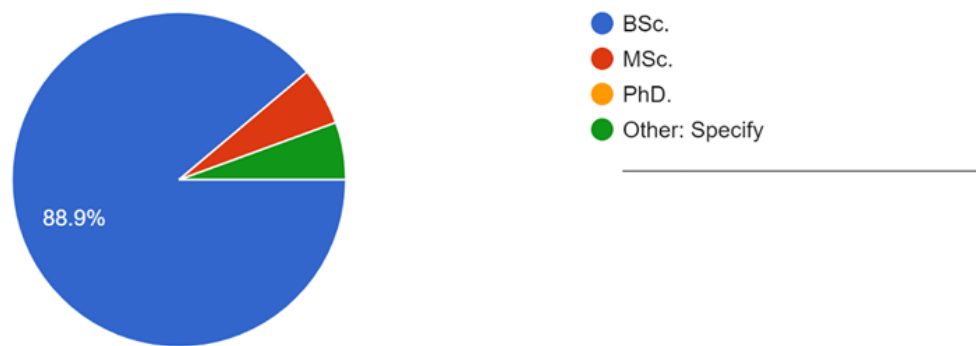


Figure 15: Interview Result – Education Level

As we can see in the previous table and figure relating to education level, the majority of respondents in this survey have a Bachelor's degree, 88.9% of them hold a Bachelor's degree, and 5.6% have a master's degree. In this survey, 5.6% of respondents hold other degrees, but the education level was not specified, so we are unable to determine if there are any PhD holders in this group.

4.2.7.9. Summary of Participants Profile

The table below provides an overall summary of the respondents' profile:

Category	Parameter	Frequency	Percentage
----------	-----------	-----------	------------

Gender	Male	62	57.4%
	Female	46	42.6%
Age	Below 30	42	38.9%
	30-39	59	54.6%
	40-49	5	4.6%
	50-59	1	0.9%
	60 and above	1	0.9%
Marital Status	Single	40	37%
	Married with children	54	50%
	Married no children	14	13%
	Other	0	0%
Education Level: University Degree	BSc.	96	88.9%
	MSc.	6	5.6%
	PhD.	0	0%
	Other	6	5.6%

Table 26: Interview Result – Summary of Respondents Profile

4.2.8. Independent and Dependent Variable Questions

In this section, the independent, moderator, and dependent variables questions are displayed, along with the interview results, in graphs. We begin with a presentation of the questions, and then we walk through the interview results for each.

According to Kaplan & Saccuzzo (2017), statistics can be divided into descriptive and inferential branches. Prior to discussing the variable questions, it is important

to note that statistical analysis is divided into two main branches. The interpretation of questionnaires, structured quantitative interviews, and hypothesizes are all based on both statistical methods. The distinction between descriptive statistics and inferential statistics can be made by looking at the diagrams, charts, and illustrations that describe each. Descriptive statistics are used to present results visually, while inferential statistics are used to draw inferences and make predictions about the larger population based on the data provided.

As Houston (2022) explains, quantitative data can also be collected through interviews; however, quantitative interviews are structured in such a way that they form closed-ended questions that do not give participants the opportunity to elaborate on the study context.

The current research comprises structured interviews in which patterns and characteristics of the data are summarized, as descriptive analysis is used to investigate employees' behavior related to cybersecurity culture. In contrast, while inferential statistics are centered around inferring relationships and patterns in data, SVM algorithms focus on selecting features, hypothesis testing, and evaluating models.

4.2.8.1. Independent Variable Questions

We measured employee behavior in this study by looking at two independent variables: External Influences (EI) and Organizational Mechanisms (OM).

Following are the questions associated with each of the independent variables:

1. External Influences (EI)

Includes 3 sub factors and 3 parameters.

Sub factor	Code	Intention	Question
------------	------	-----------	----------

Societal Cybersecurity Culture	EI1	Culture and society of the country or region in which the bank is located	Could Bahraini society have an impact on cybersecurity cultural backgrounds within your organization?
External Rules and Regulations	EI2	The role of government and central bank laws, guidelines, and regulations	In your opinion, do government policies and regulations have an impact on organizational cybersecurity culture?
Peer Institution	EI3	Peer Institutions	Is it necessary for top management to always know the level of cyber security adoption at other organizations?

Table 27: Independent Variable Questions – External Influences

2. Organizational Mechanisms (OM)

Includes 7 sub factors and 7 parameters.

Sub factor	Code	Intention	Question
Cybersecurity Culture Leadership	OM1	Individual or team who is responsible for fostering a cybersecurity culture	Do you think that a leader is essential for building a cybersecurity culture in the organization?
Performance Evaluations	OM2	The importance of regular formal evaluations for employees	Are you of the opinion that employee behavior evaluations in regards to cybersecurity are able to identify employees' strengths

			and weaknesses, and that this can result in a significant change in their behavior?
Rewards and Punishments	OM3	An analysis of the managerial impacts of cybersecurity behavior.	Have you seen that employee cybersecurity behavior is significantly affected by reward and punishment?
Organizational Learning	OM4	The different ways that the organization builds, retains, and improves its cybersecurity knowledge.	Are you convinced that establishing different formal and informal organizational channels that support or engage employees in cybersecurity has a positive impact?
Cybersecurity Training	OM5	Employee training and development in cybersecurity	What do you think about the fact that different training programs and tools can significantly affect employee awareness, knowledge, and behavior regarding cybersecurity among employees?
Communications Channel	OM6	Develop multiple channels for cybersecurity delivery	Can various channels to convey the significance of cybersecurity, such as videos, training, or emails, help to

			improve employee behavior regarding cybersecurity?
Budget	OM7	Investing in cybersecurity properly and positively	Is it your belief that management expects positive results in employees' security behavior by allocating properly cyber security budgets?

Table 28: Independent Variable Questions – Organizational Mechanisms

4.2.8.2. Moderating Variable Questions

In this study, we measured employee behavior and intention to behave by considering the organization's cybersecurity culture as a moderator variable.

In connection with the moderator variable, the following questions were asked:

Sub factor	Code	Intention	Question
Top Management's Participation	CSC1	Management's involvement in establishing a cybersecurity culture by focusing on the individuals, groups and organizational characteristics.	Developing a cyber-culture that integrates external collaboration with a positive internal culture that includes individual, group, and organizational characteristics is essential for achieving the desired employee cybersecurity behavior, according to you?

Community Norms and Beliefs	CSC2	Different Communities can result in different ideas and norms that impact cybersecurity culture in an organization	Religious, family, and social influences play a significant role in employee beliefs and values when it comes to cybersecurity?
Top Management's Priorities	CSC3	The cybersecurity culture is determined by decision leaders	Does your institution's management make efforts to raise security awareness among employees in various ways?
Top Management's Participation	CSC4	Regulating or policies that decision makers impose relating to cybersecurity	Is it possible to encourage employees in banking sector to develop their security behavior by making cybersecurity programs and a cybersecurity culture mandatory?
Top Management's Participation	CSC5	A lack of involvement of cybersecurity decision makers	The Board of Directors of your institution is not involved in cybersecurity-related activities?
Top Management's knowledge	CSC6	Deficiencies in cybersecurity knowledge among decision makers	The board of directors frequently takes no role regarding important initiatives, which include security

			strategy, budget, and risk assessment.
Top Management's Priorities	CSC7	Strategic priorities and cybersecurity culture at the top of organizations	At your institution, have the executives given cybersecurity a strategic priority? As an example, they allocated considerable budgets for security activities, tools, and professionals.
Top Management's Participation	CSC8	Discussions in groups and individually by top management around cybersecurity topics	In order to keep their knowledge current, does your top management regularly discuss cybersecurity topics as a part of their leadership team meetings and individually with cyber experts?
Teamwork Perception	CSC9	A culture of cybersecurity is shaped by teamwork	If your institution provides teamwork among its employees, would it help them to compare notes about phishing exercises and discuss other cyber-related topics?
General Cyber Threat Awareness	CSC10	Cybersecurity awareness of employees by their age group	Compared to younger employees, older adults display higher levels of

			awareness and proficiency with cybersecurity.
General Cyber Threat Awareness	CSC11	Considering employees' gender in the context of cybersecurity awareness	Do females score lower than males for security awareness and ability in your institution?
Employee's Self-Efficacy	CSC12	How employee self-belief affects cybersecurity	In your institution, have you noticed that employees with a similar level of awareness of cybersecurity are more likely to grasp its concepts than others without such experience?
Cybersecurity Policy Awareness	CSC13	Behavior of employees based on their understanding of cybersecurity policies	One goal of a cybersecurity organizational culture is to influence the behavior of staff with respect to complying with the official security policy.
Cybersecurity Policy Awareness	CSC14	Behaviors of employees in relation to cybersecurity culture	The cyber culture of an organization can improve security behavior among employees.

4.2.8.3. Dependent Variable Questions

This study concluded with questions about intention and cybersecurity behavior for each interviewee based on cybersecurity culture.

The following questions were asked regarding the dependent variables:

Sub factor	Code	Intention	Question
Cybersecurity Training and Intention	BI1	Intention of employees to follow cybersecurity training	Upon completion of the cybersecurity training, did employees declare their intention to follow all policies and practices at work?
Cybersecurity Policy and Intention	BI2	An employee's intention to improve cybersecurity	Is the employee intent to follow the cybersecurity policy in order to improve the organization's cybersecurity in regard to future IT activities after receiving the required security training or courses from your institution?
External Cybersecurity	BI3	Encouragement of cybersecurity by employees	It has been observed that employees tend to encourage their friends and colleagues to utilize cybersecurity practices after the completion of training courses?
Cybersecurity culture and intention	BI4	Effects of cyber security culture on employees' compliance intentions	It is evident that employee attitudes, beliefs, and values have a significant effect on whether employees intend to

			comply with cybersecurity policy requirements.
Cybersecurity Training and Behavior	CSB1	Employee behavior after cybersecurity training	Since the employees are through the cybersecurity training, employees gained a deeper understanding of cybersecurity and displayed improved security behavior.
Awareness programs and cybersecurity behavior	CSB2	Behaviors of employees in relation to cybersecurity awareness programs	Many cybersecurity awareness programs fail to educate the users on why security is important and fail to motivate the users to change their behavior.
Cybersecurity awareness, training, and education	CSB3	Education, awareness, and training in cybersecurity	Changing behavior toward security requires a broader approach to security awareness, training, and education than annual computer-based trainings.
Cybersecurity behavior and Facilitating Conditions	CSB4	Involvement of facilitating conditions in employee behavior and compliance	As a result of compliance, employees present more impressive cybersecurity behaviors in the organization.

4.2.8.4. Summary of All Variable Questions

The following is a table that summarizes all the variable questions and their code:

Independent Variable – External Influences (EI)			
Sub factor	Code	Intention	Question
Societal Cybersecurity Culture External Rules and Regulations Peer Institution	EI1	Culture and society of the country or region in which the bank is located	Could Bahraini society have an impact on cybersecurity cultural backgrounds within your organization?
	EI2	The role of government and central bank laws, guidelines, and regulations	In your opinion, do government policies and regulations have an impact on organizational cybersecurity culture?
	EI3	Comparative level of peer organizations	Is it necessary for top management to always know the level of cyber security adoption at other organizations?
Societal Cybersecurity Culture External Rules and Regulations Peer Institution	EI1	Culture and society of the country or region in which the bank is located	Could Bahraini society have an impact on cybersecurity cultural backgrounds within your organization?
	EI2	The role of government and central bank laws,	In your opinion, do government policies and regulations have an impact on

		guidelines, and regulations	organizational cybersecurity culture?
	EI3	Comparative level of peer organizations	Is it necessary for top management to always know the level of cyber security adoption at other organizations?
Independent Variables – Organizational Mechanisms (OM)			
Sub factor	Code	Intention	Question
Cybersecurity Culture Leadership	OM1	Individual or team who is responsible for fostering a cybersecurity culture	Do you think that a leader is essential for building a cybersecurity culture in the organization?
Performance Evaluations	OM2	The importance of regular formal evaluations for employees	Are you of the opinion that employee behavior evaluations in regards to cybersecurity are able to identify employees' strengths and weaknesses, and that this can result in a significant change in their behavior?
Rewards and Punishments	OM3	An analysis of the managerial impacts of cybersecurity behavior.	Have you seen that employee cybersecurity behavior is significantly affected by reward and punishment?

Organizational Learning	OM4	The different ways that the organization builds, retains, and improves its cybersecurity knowledge.	Are you convinced that establishing different formal and informal organizational channels that support or engage employees in cybersecurity has a positive impact?
Cybersecurity Training	OM5	Employee training and development in cybersecurity	What do you think about the fact that different training programs and tools can significantly affect employee awareness, knowledge, and behavior regarding cybersecurity among employees?
Communications Channel	OM6	Develop multiple channels for cybersecurity delivery	Can various channels to convey the significance of cybersecurity, such as videos, training, or emails, help to improve employee behavior regarding cybersecurity?
Budget	OM7	Investing in cybersecurity properly and positively	Is it your belief that management expects positive results in employees' security behavior by allocating

			properly cyber security budgets?
Moderating Variable – Cybersecurity Culture (CSC)			
Sub factor	Code	Intention	Question
Top Management's Participation	CSC1	Management's involvement in establishing a cybersecurity culture by focusing on the individuals, groups and organizational characteristics.	Developing a cyber-culture that integrates external collaboration with a positive internal culture that includes individual, group, and organizational characteristics is essential for achieving the desired employee cybersecurity behavior, according to you?
Community Norms and Beliefs	CSC2	Different Communities can result in different ideas and norms that impact cybersecurity culture in an organization	Religious, family, and social influences play a significant role in employee beliefs and values when it comes to cybersecurity?
Top Management's Priorities	CSC3	The cybersecurity culture is determined by decision leaders	Does your institution's management make efforts to raise security awareness among employees in various ways?

Top Management's Participation	CSC4	Regulating or policies that decision makers impose relating to cybersecurity	Is it possible to encourage employees in banking sector to develop their security behavior by making cybersecurity programs and a cybersecurity culture mandatory?
Top Management's Participation	CSC5	A lack of involvement of cybersecurity decision makers	The Board of Directors of your institution is not involved in cybersecurity-related activities?
Top Management's knowledge	CSC6	Deficiencies in cybersecurity knowledge among decision makers	The board of directors frequently takes no role regarding important initiatives, which include security strategy, budget, and risk assessment.
Top Management's Priorities	CSC7	Strategic priorities and cybersecurity culture at the top of organizations	At your institution, have the executives given cybersecurity a strategic priority? As an example, they allocated considerable budgets for security activities, tools, and professionals.

Top Management's Participation	CSC8	Discussions in groups and individually by top management around cybersecurity topics	In order to keep their knowledge current, does your top management regularly discuss cybersecurity topics as a part of their leadership team meetings and individually with cyber experts?
Teamwork Perception	CSC9	A culture of cybersecurity is shaped by teamwork	If your institution provides teamwork among its employees, would it help them to compare notes about phishing exercises and discuss other cyber-related topics?
General Cyber Threat Awareness	CSC10	Cybersecurity awareness of employees by their age group	Compared to younger employees, older adults display higher levels of awareness and proficiency with cybersecurity.
General Cyber Threat Awareness	CSC11	Considering employees' gender in the context of cybersecurity awareness	Do females score lower than males for security awareness and ability in your institution?
Employee's Self-Efficacy	CSC12	How employee self-belief affects cybersecurity	In your institution, have you noticed that employees with a similar level of awareness of cybersecurity are more likely to

			grasp its concepts than others without such experience?
Cybersecurity Policy Awareness	CSC13	Behavior of employees based on their understanding of cybersecurity policies	One goal of a cybersecurity organizational culture is to influence the behavior of staff with respect to complying with the official security policy.
Cybersecurity Policy Awareness	CSC14	Behaviors of employees in relation to cybersecurity culture	The cyber culture of an organization can improve security behavior among employees.
Dependent Variables – Behavior Intention (BI) and Cybersecurity Behavior (CSB)			
Sub factor	Code	Intention	Question
Cybersecurity Training and Intention	BI1	Intention of employees to follow cybersecurity training	Upon completion of the cybersecurity training, did employees declare their intention to follow all policies and practices at work?
Cybersecurity Policy and Intention	BI2	An employee's intention to improve cybersecurity	Is the employee intent to follow the cybersecurity policy in order to improve the organization's cybersecurity in regard to future IT activities after receiving the required

			security training or courses from your institution?
External Cybersecurity	BI3	Encouragement of cybersecurity by employees	It has been observed that employees tend to encourage their friends and colleagues to utilize cybersecurity practices after the completion of training courses?
Cybersecurity culture and intention	BI4	Effects of cyber security culture on employees' compliance intentions	It is evident that employee attitudes, beliefs, and values have a significant effect on whether employees intend to comply with cybersecurity policy requirements.
Cybersecurity Training and Behavior	CSB1	Employee behavior after cybersecurity training	Since the employees are through the cybersecurity training, employees gained a deeper understanding of cybersecurity and displayed improved security behavior.
Awareness programs and cybersecurity behavior	CSB2	Behaviors of employees in relation to cybersecurity awareness programs	Many cybersecurity awareness programs fail to educate the users on why security is important and fail to motivate

			the users to change their behavior.
Cybersecurity awareness, training, and education	CSB3	Education, awareness, and training in cybersecurity	Changing behavior toward security requires a broader approach to security awareness, training, and education than annual computer-based trainings.
Cybersecurity behavior and Facilitating Conditions	CSB4	Involvement of facilitating conditions in employee behavior and compliance	As a result of compliance, employees present more impressive cybersecurity behaviors in the organization.

Table 29: Summary of All Variable Questions

4.2.8.5. Interview Results of Variable Questions

Following are all the results acquired from the interviews represented in graphs, each question will be presented, and the graph related to the question holding the responses of the participants will follow it:

- The following figures show the descriptive analysis of the interviews:

Section EI: External Influences

EI1 - Could Bahraini society have an impact on cybersecurity cultural backgrounds within your organization?

108 responses

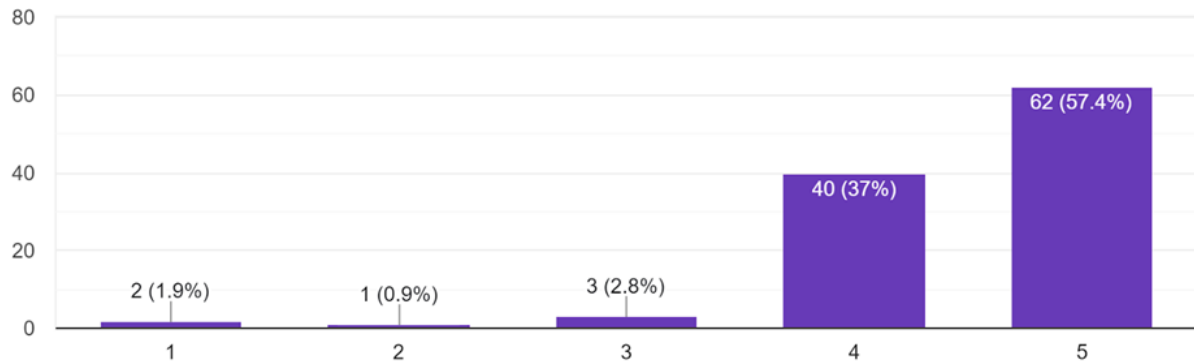


Figure 16: Interview Result – EI1

EI2 - In your opinion, do government policies and regulations have an impact on organizational cybersecurity culture?

108 responses

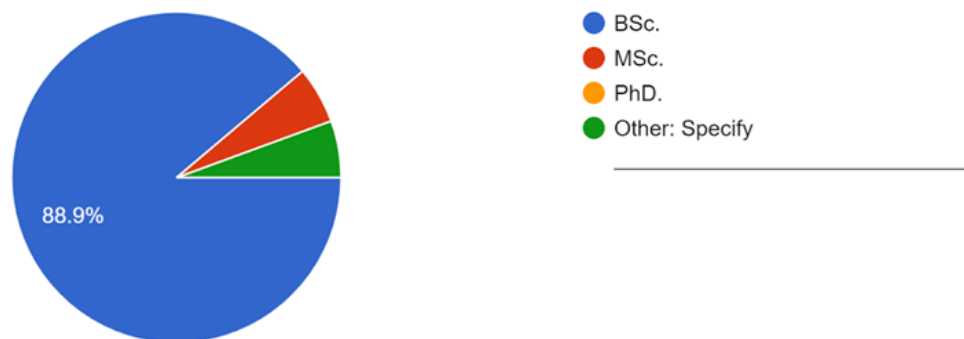


Figure 17: Interview Result – EI2

EI3 - Is it necessary for top management to always know the level of cyber security adoption at other organizations?

108 responses

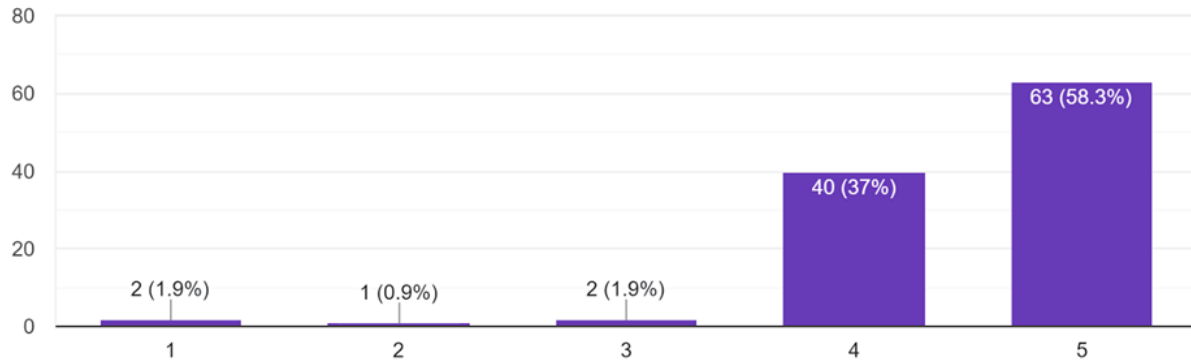


Figure 18: Interview Result – EI2

Section OM: Organizational Mechanisms

OM1 - Do you think that a leader is essential for building a cybersecurity culture in the organization?

108 responses

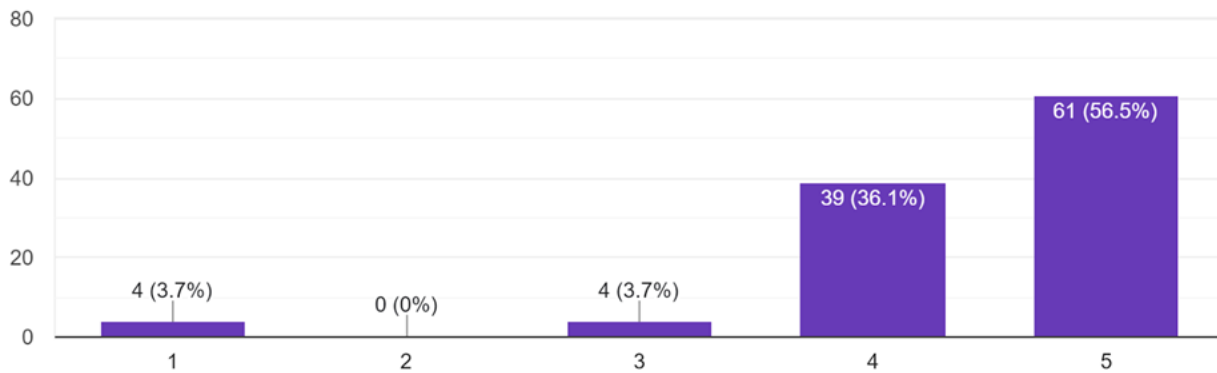


Figure 19: Interview Result – OM1

OM2 - Are you of the opinion that employee behavior evaluations in regards to cybersecurity are able to identify employees' strengths and weaknesses, and that this can result in a significant change in their behavior?

108 responses

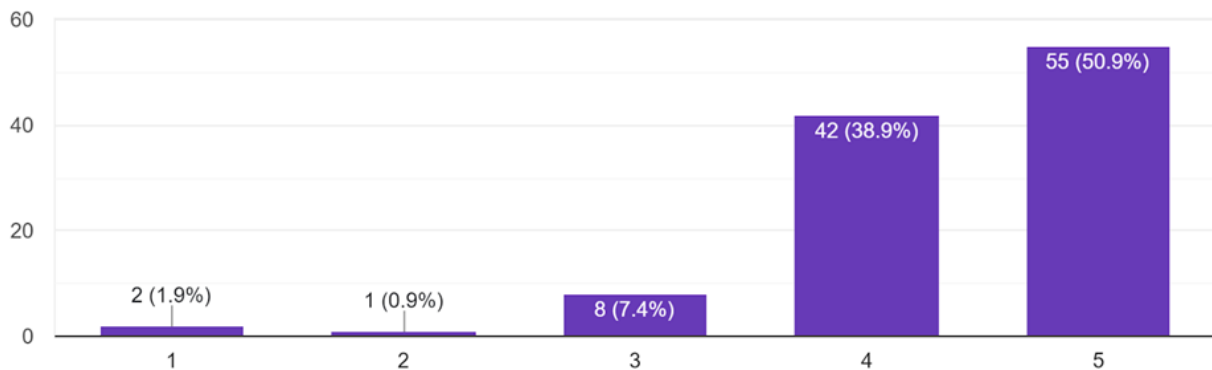


Figure 20: Interview Result – OM2

OM4 - Are you convinced that establishing different formal and informal organizational channels that support or engage employees in cybersecurity has a positive impact

108 responses

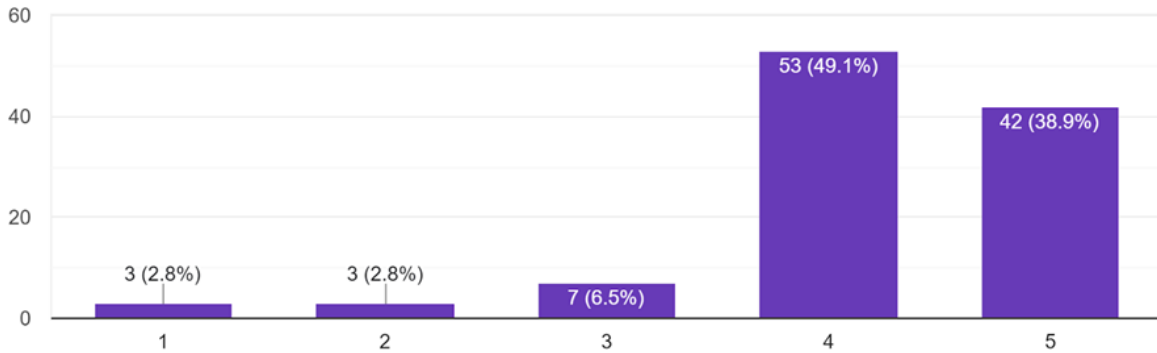


Figure 21: Interview Result – OM4

OM5 - What do you think about the fact that different training programs and tools can significantly affect employee awareness, knowledge, and behavior regarding cybersecurity among employees?

108 responses

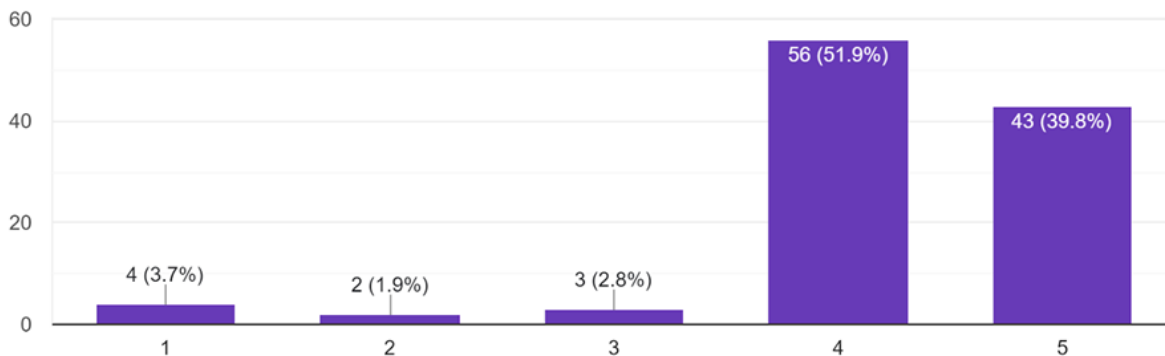


Figure 22: Interview Result – OM5

OM7- Is it your belief that management expects positive results in employees' security behavior by allocating properly cyber security budgets?

108 responses

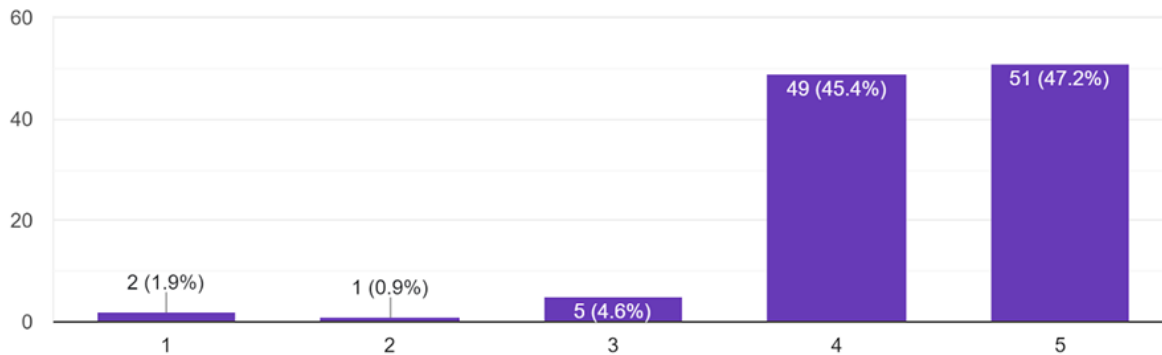


Figure 23: Interview Result – OM7

4.2.8.5. Interview Results of Variable Questions

Section CSC: Cybersecurity Culture

CSC1- Developing a cyber-culture that integrates external collaboration with a positive internal culture that includes individual, group, and organizational characteristics is essential for achieving the desired employee cybersecurity behavior, according to you?

108 responses

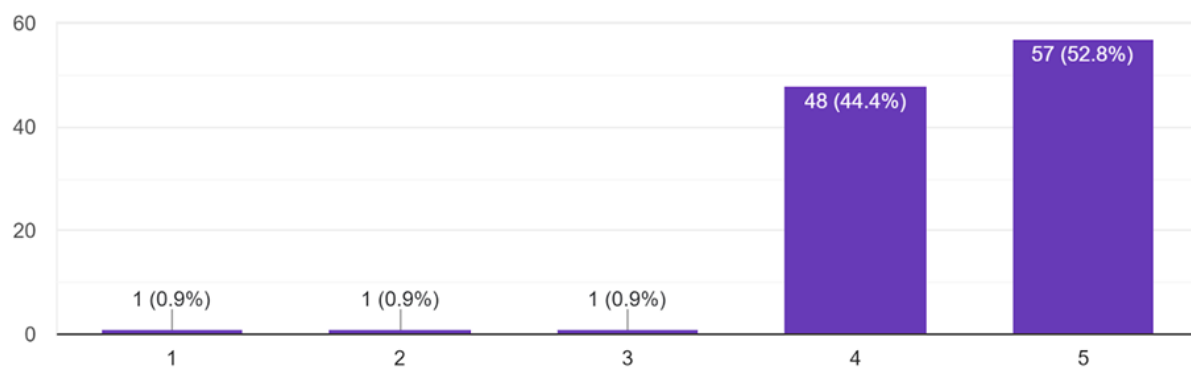


Figure 24: Interview Result – CSC1

CSC2- Religious, family, and social influences play a significant role in employee beliefs and values when it comes to cybersecurity?

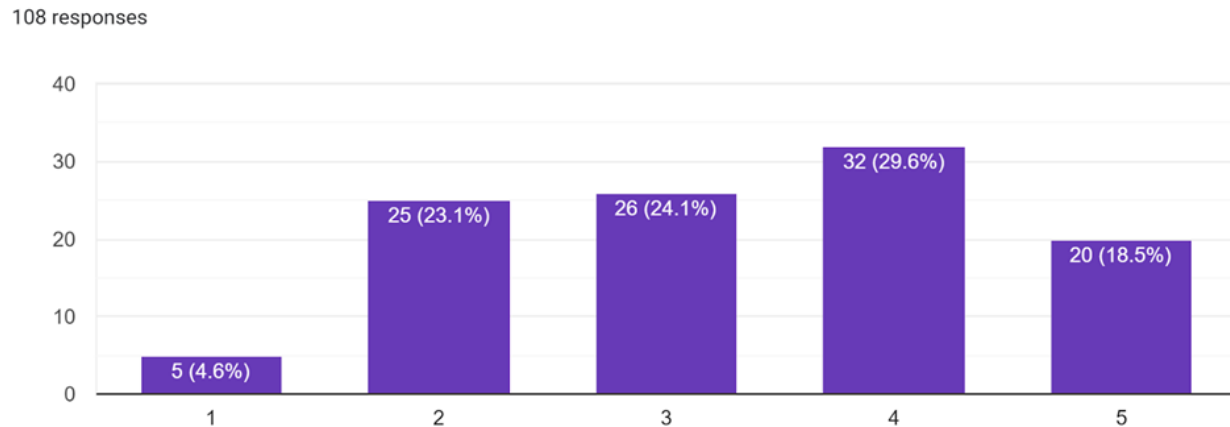


Figure 25: Interview Result – CSC2

CSC3- Does your institution's management make efforts to raise security awareness among employees in various ways?

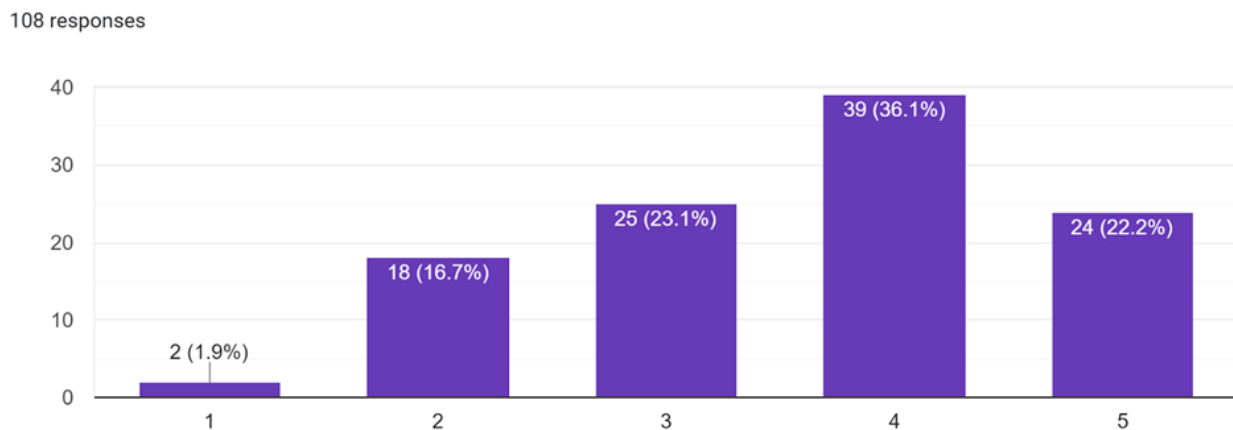


Figure 26: Interview Result – CSC3

CSC4- Is it possible to encourage employees in banking sector to develop their security behavior by making cybersecurity programs and a cybersecurity culture mandatory?

108 responses

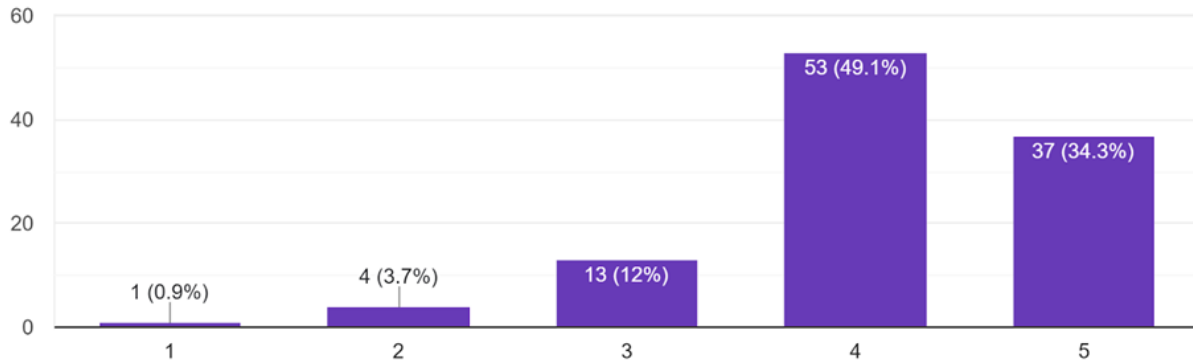


Figure 27: Interview Result – CSC4

CSC5- The Board of Directors of your institution is not involved in cybersecurity-related activities?

108 responses

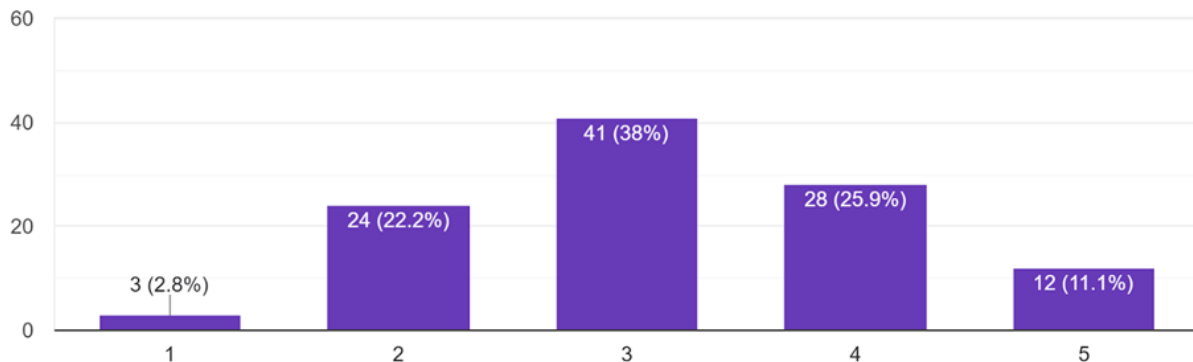


Figure 28: Interview Result – CSC5

CSC6- The board of directors frequently takes no role regarding important initiatives, which include security strategy, budget, and risk assessment.

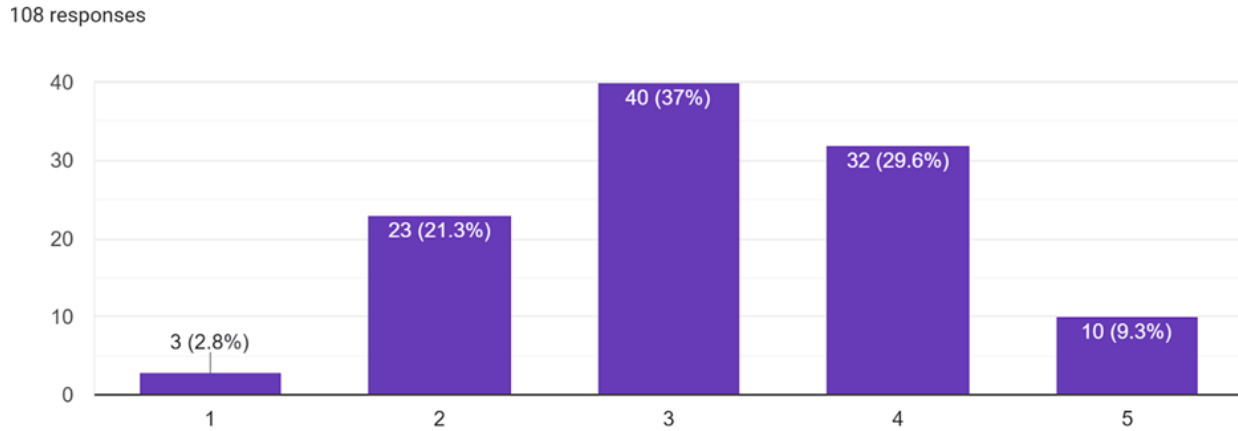


Figure 29: Interview Result – CSC6

CSC7- At your institution, have the executives given cybersecurity a strategic priority? As an example, they allocated considerable budgets for security activities, tools, and professionals.

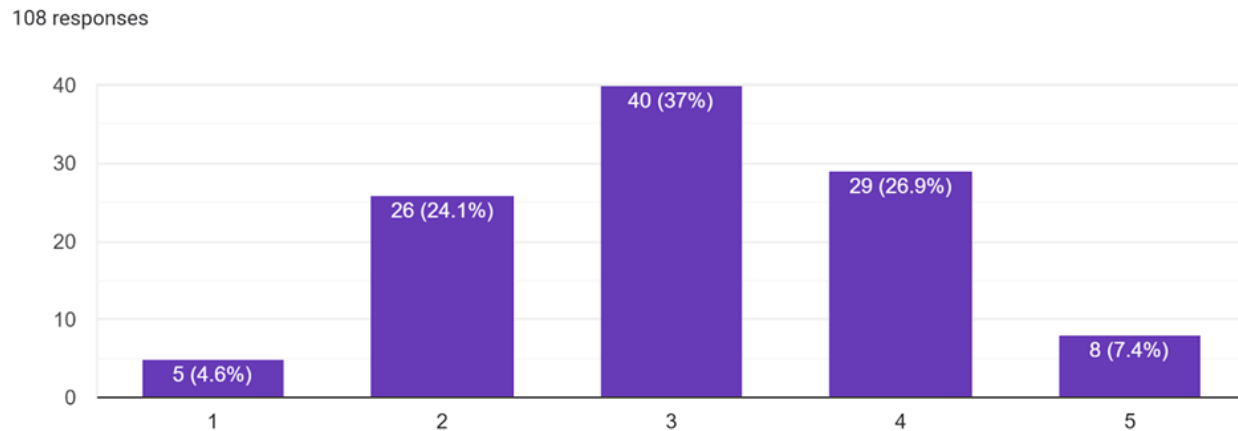


Figure 30: Interview Result – CSC7

CSC8- In order to keep their knowledge current, does your top management regularly discuss cybersecurity topics as a part of their leadership team meetings and individually with cyber experts?

108 responses

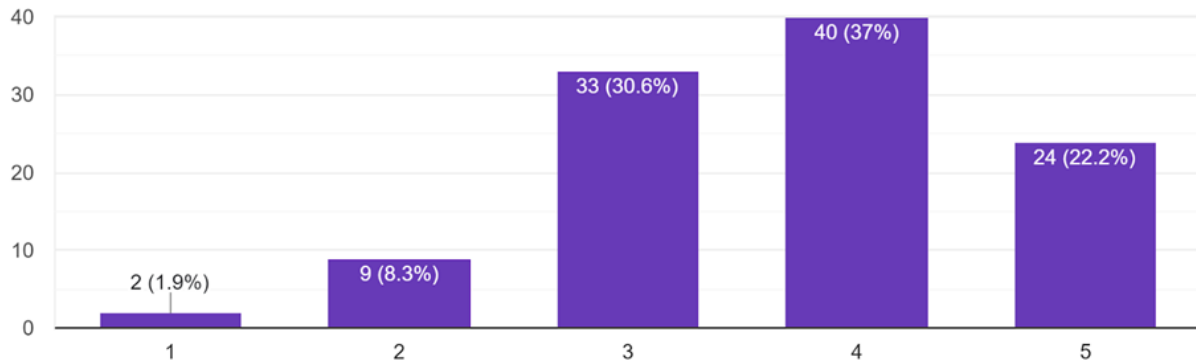


Figure 31: Interview Result – CSC8

CSC9- If your institution provides teamwork among its employees, would it help them to compare notes about phishing exercises and discuss other cyber-related topics?

108 responses

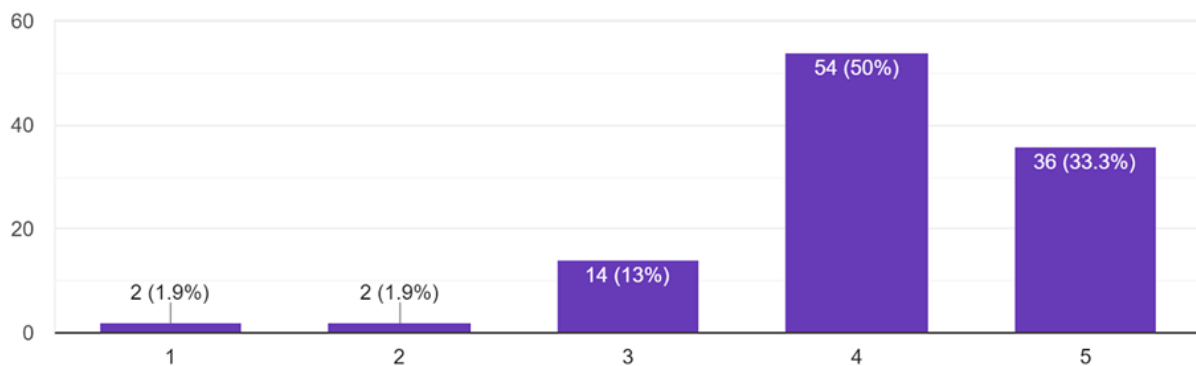


Figure 32: Interview Result – CSC9

CSC10- Compared to younger employees, older adults display higher levels of awareness and proficiency with cybersecurity.

108 responses

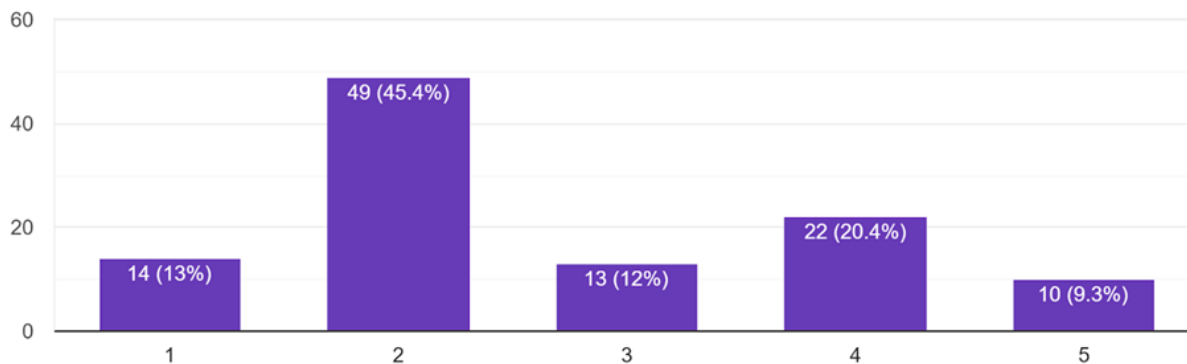


Figure 33: Interview Result – CSC10

CSC11- Do females score lower than males for security awareness and ability in your institution?

108 responses

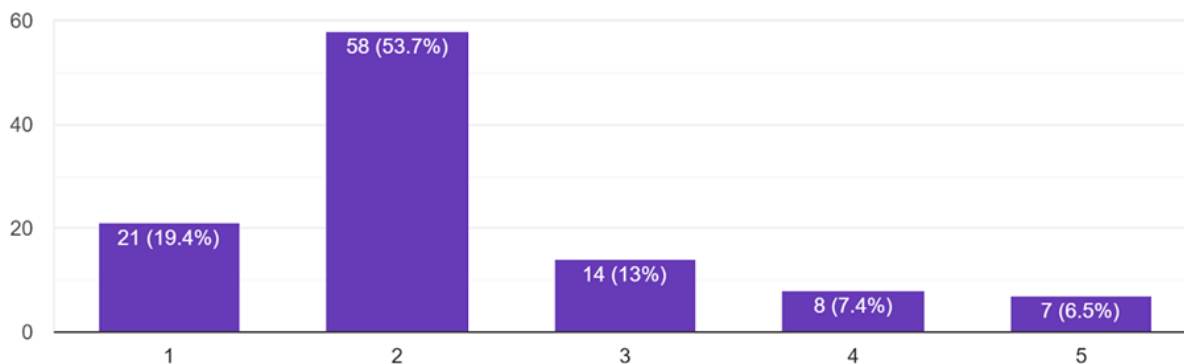


Figure 34: Interview Result – CSC11

CSC12- In your institution, have you noticed that employees with a similar level of awareness of cybersecurity are more likely to grasp its concepts than others without such experience?

108 responses

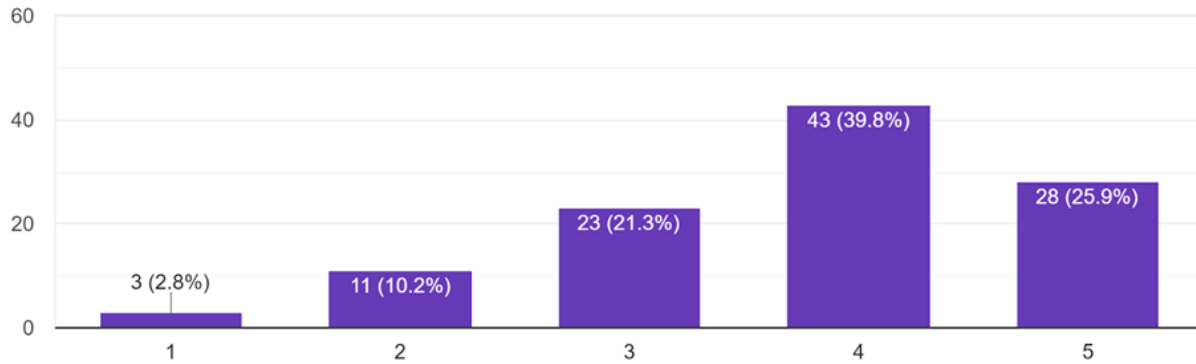


Figure 35: Interview Result – CSC12

CSC13- One goal of a cybersecurity organizational culture is to influence the behavior of staff with respect to complying with the official security policy.

108 responses

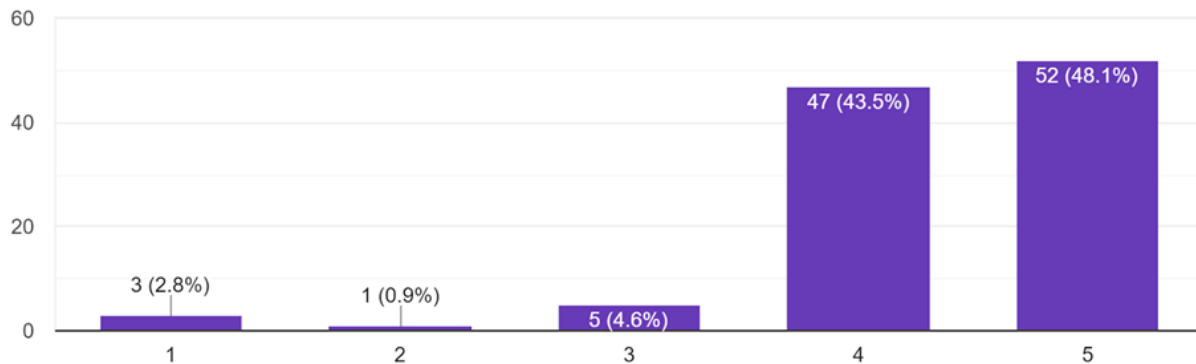


Figure 36: Interview Result – CSC13

CSC14- The cyber culture of an organization can improve security behavior among employees.

108 responses

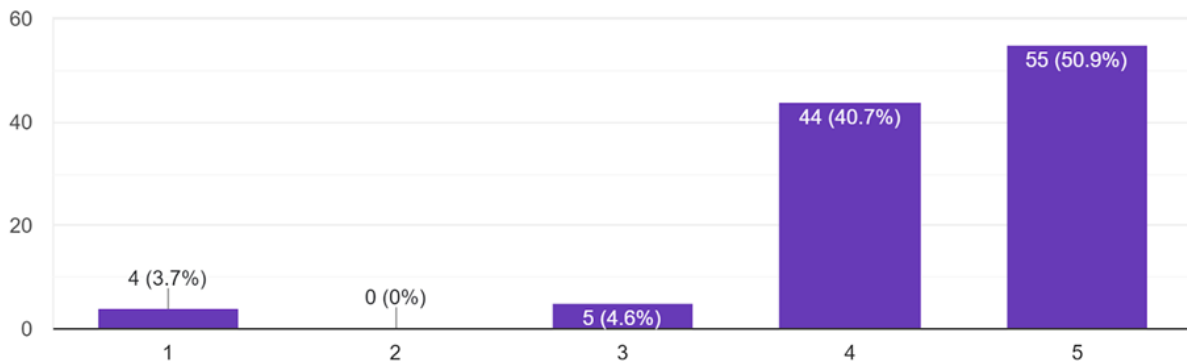


Figure 37: Interview Result – CSC14

4.2.8.6. Interview Results of Dependent Variable Questions

Section BI: Behavior Intention

BI1- Upon completion of the cybersecurity training, did employees declare their intention to follow all policies and practices at work?

108 responses

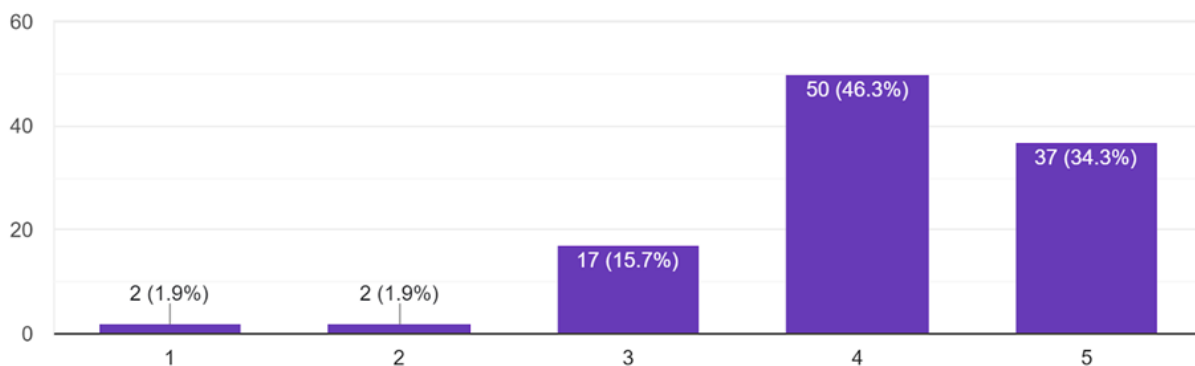


Figure 38: Interview Result – BI1

BI2- Is the employee intent to follow the cybersecurity policy in order to improve the organization's cybersecurity in regard to future IT activities after receiving the required security training or courses from your institution?

108 responses

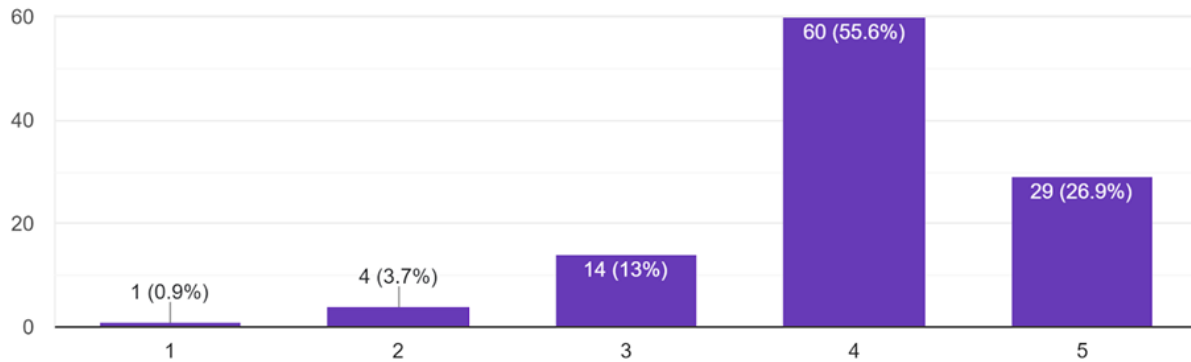


Figure 39: Interview Result – BI2

BI3- It has been observed that employees tend to encourage their friends and colleagues to utilize cybersecurity practices after the completion of training courses?

108 responses

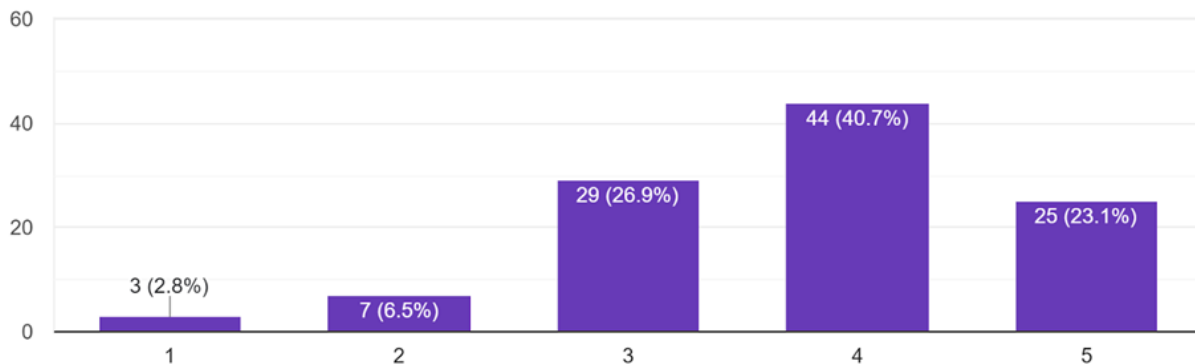


Figure 40: Interview Result – BI3

BI4- It is evident that employee attitudes, beliefs, and values have a significant effect on whether employees intend to comply with cybersecurity policy requirements.

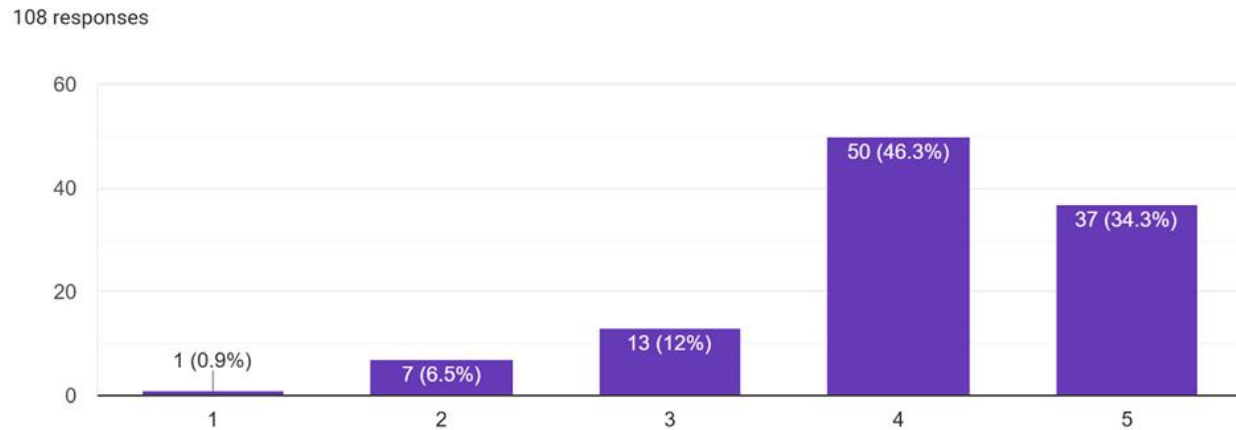


Figure 41: Interview Result – BI4

Section CSB: Cybersecurity Behavior

CSB1- Since the employees are through the cybersecurity training, employees gained a deeper understanding of cybersecurity and displayed improved security behavior.

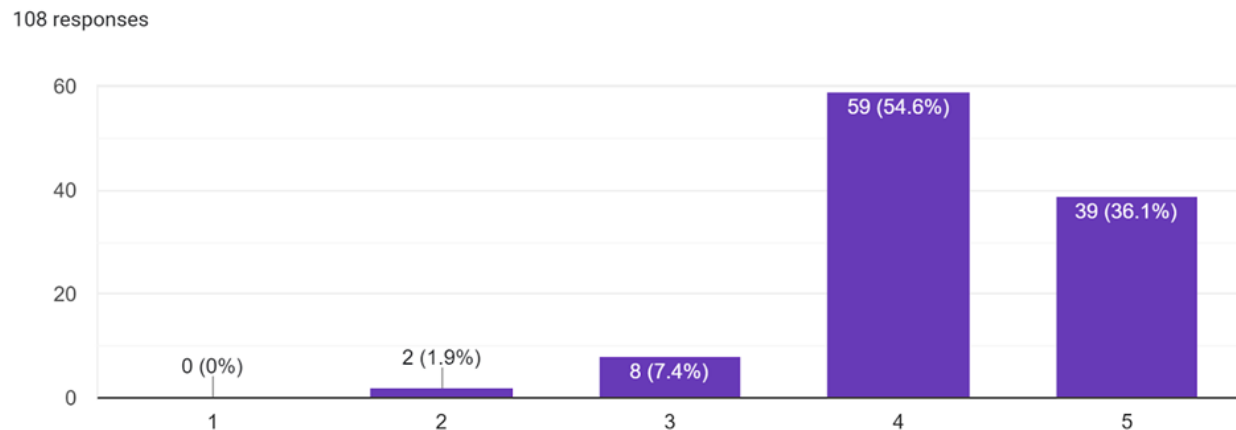


Figure 42: Interview Result – CSB1

CSB2- Many cybersecurity awareness programs fail to educate the users on why security is important and fail to motivate the users to change their behavior.

108 responses

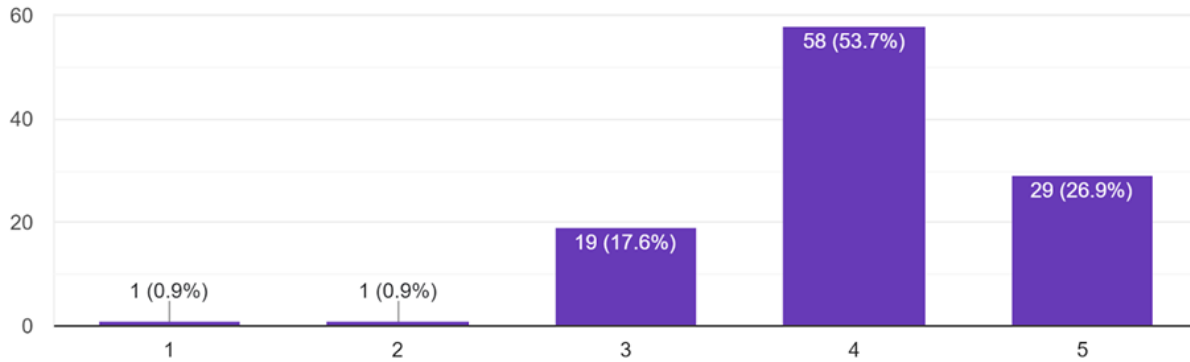


Figure 43: Interview Result – CSB2

CSB3- Changing behavior toward security requires a broader approach to security awareness, training, and education than annual computer-based trainings.

108 responses

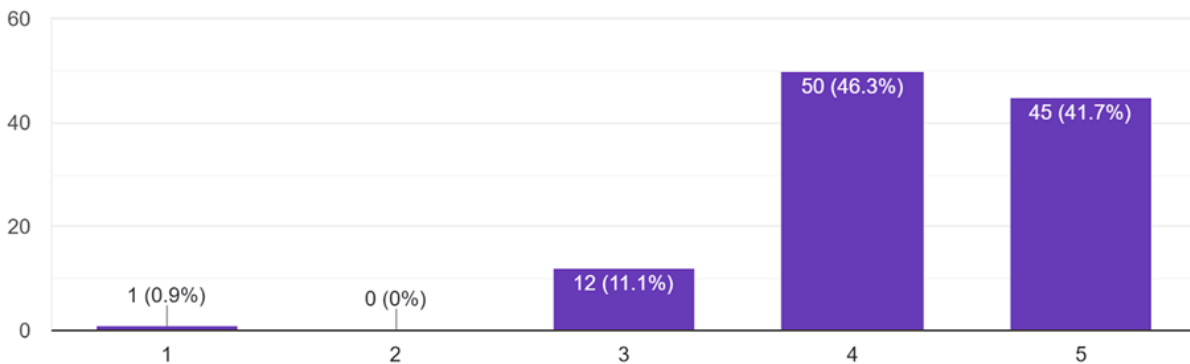


Figure 44: Interview Result – CSB3

CSB4- As a result of compliance, employees present more impressive cybersecurity behaviors in the organization.

108 responses

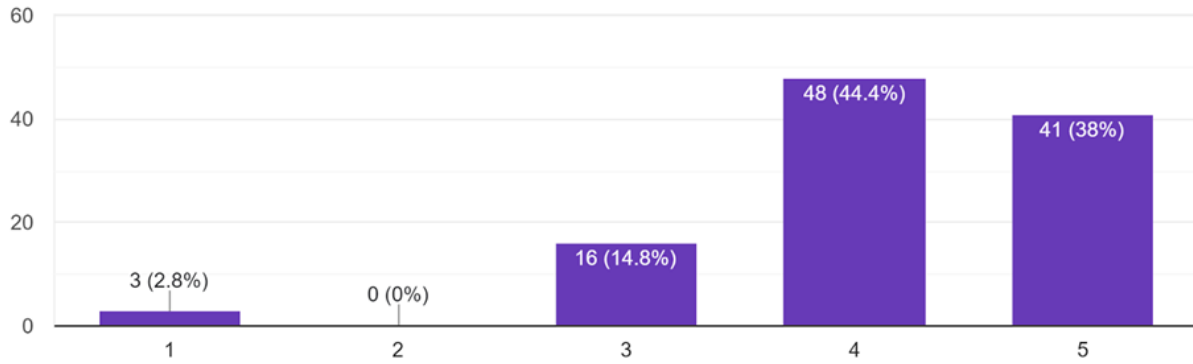


Figure 45: Interview Result – CSB4

CSB5- Facilitating conditions can affect the intention to use and behavior use.

108 responses

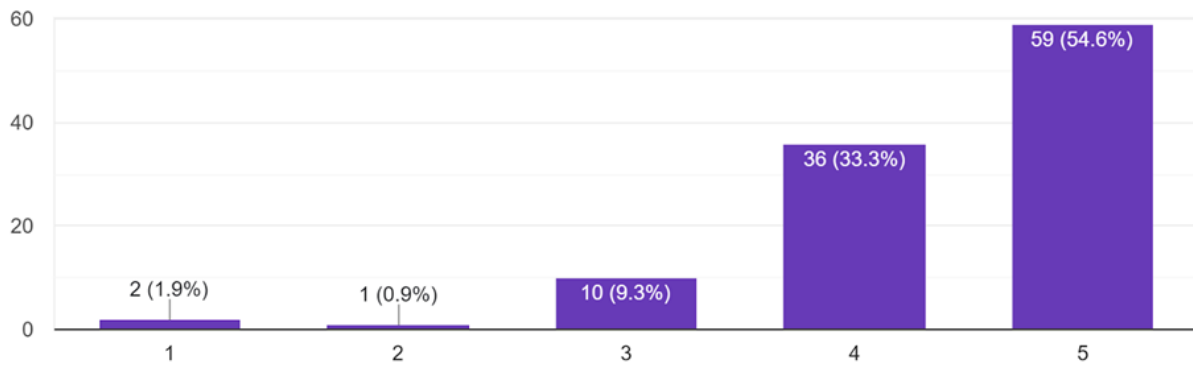


Figure 46: Interview Result – CSB5

4.3. Analysis: The Machine Learning Pipeline

The analysis in this section demonstrates how the findings were used in the machine learning pipeline in conjunction with the Support Vector Machines algorithm.

4.3.1. Dataset Collection

The data is acquired from interviews conducted on a sample of 108 participants. The interviews included structured close-ended questions, that were categorized and coded for utilization in descriptive analysis. The questions of the interview are extracted from a previous literature study and adjusted for the current study. The interviewing process included a clear agenda, structured questions and was done on a one-on-one basis, both online and in-person. The number of interviewers consisted of four (4) members, 3 of whom were trained by the researcher of this paper, and the researcher is the 4th member in the team. The data is inserted into the Google Forms Online Platform, and it was used as the data input system to effectively avoid input of incorrect data by the interviewers during the interview.

The data, once the target sample has been reached, is then extracted from Google Forms via the use of the Microsoft Excel Sheet Program, and it has been thoroughly reviewed by the researcher for the purpose of cleaning, ensuring all values are available, no questions were missed and to acquire a 100% participation rate.

Figure 67 shows the data in an excel sheet:

	A	B	C	D	E	F	G	H	I	J
1	Timestamp	Gender	Age	Marital Status	Education Level: Unive	Field of study	EI1) Could Bahraini so	EI2) In your opinion, d	EI3) Is it necessary fo	OM1) Do you think th
2	2/11/2023 0:26:04	Female	30-39	Married with children	BSc.	Science	5	5	5	5
3	2/11/2023 20:24:03	Female	30-39	Married with children	Other: Specify _____	Business	5	4	5	5
4	2/11/2023 21:04:46	Female	30-39	Married with children	BSc.	Business	4	2	5	5
5	2/12/2023 3:14:57	Male	Below 30	Single	BSc.	Business	5	4	5	5
6	3/1/2023 13:07:03	Female	Below 30	Single	BSc.	Business	4	4	4	5
7	3/1/2023 18:01:54	Female	Below 30	Married no children	MSc.	Business	2	2	1	1
8	3/6/2023 15:23:56	Male	50-59	Married with children	Other: Specify _____	Business	4	4	5	5
9	3/10/2023 21:50:49	Female	Below 30	Single	Other: Specify _____	Business	4	1	5	3
10	10/27/2023 21:43:03	Female	Below 30	Single	BSc.	Business	3	3	3	3
11	10/27/2023 21:58:24	Female	Below 30	Single	BSc.	Science	4	5	5	5
12	10/27/2023 23:18:36	Female	Below 30	Single	BSc.	Other: Specify _____	5	5	5	5
13	10/27/2023 23:26:52	Female	60 and above	Married with children	Other: Specify _____	Business	4	3	5	3
14	10/28/2023 19:50:41	Female	Below 30	Single	BSc.	Business	1	4	5	1
15	11/2/2023 10:14:49	Female	Below 30	Single	BSc.	Science	3	3	2	5
16	11/11/2023 19:01:52	Female	Below 30	Single	BSc.	Engineering	5	5	5	5
17	11/16/2023 0:48:07	Female	Below 30	Single	BSc.	Engineering	4	3	3	3
18	11/19/2023 8:00:50	Female	30-39	Married with children	BSc.	Science	1	1	1	1
19	11/19/2023 18:06:40	Male	30-39	Married with children	BSc.	Science	5	5	5	5
20	11/19/2023 18:09:34	Male	30-39	Married with children	BSc.	Science	5	5	5	5
21	11/20/2023 8:58:23	Male	30-39	Married with children	BSc.	Science	5	5	5	5
22	11/20/2023 9:01:27	Male	Below 30	Single	BSc.	Science	5	5	5	5

Figure 47: Interviews Data in Excel Sheet Program

According to the previous figure, the data was first extracted from the Google Sheets data input system the interviewers used during the interviews to input the data, which would be reviewed by the researcher.

4.3.2. Data Preparation

Data is collected, modified, and then prepared for machine learning in a way that is compatible with the Anaconda program as soon as it is collected. In the next step, the machine will be trained on a sample of the dataset before entering the entire dataset. Categorization will allow the machine to comprehend the variables of the study.

Input datasets for the machine learning pipeline are shown below:

Data preparation

```
In [6]: dataset.head()
```

```
Out[6]:
```

	Gender	Age	Marital Status	Education Level	Field of study	Your job Title
0	Female	30-39	Married with children	BSc.	Science	Other: Specify
1	Female	30-39	Married with children	Other: Specify	Business	Other: Specify
2	Female	30-39	Married with children	BSc.	Business	Other: Specify
3	Male	Below 30	Single	BSc.	Business	Other: Specify
4	Female	Below 30	Single	BSc.	Business	Other: Specify

5 rows × 43 columns

Figure 48: Interviews Data Input in the Machine Learning Pipeline

Using the Python programming language, the data is imported into the machine learning pipeline during the initial stages of the pipeline. Machine learning generates the input data information automatically, as shown in the previous figure. This is done during the initial stages of the pipeline. A researcher then verifies the data to ensure it is correct and flawless.

An investigation of the missing values is conducted, adjustments are made, and the dataset description is inserted. The researcher also ensures that the data has been imported from the spreadsheet program, as well as double checking if the

importing process has not caused any errors. During the data preparation process, this step is essential to ensure high accuracy and error-free results.

In order to ensure that the data is input by Python correctly, a code has been written in the machine to create graphs that show the input values for each variable that affects cybersecurity. Below is a sample of the output:

A. Values of External Influences and Organizational Mechanism.

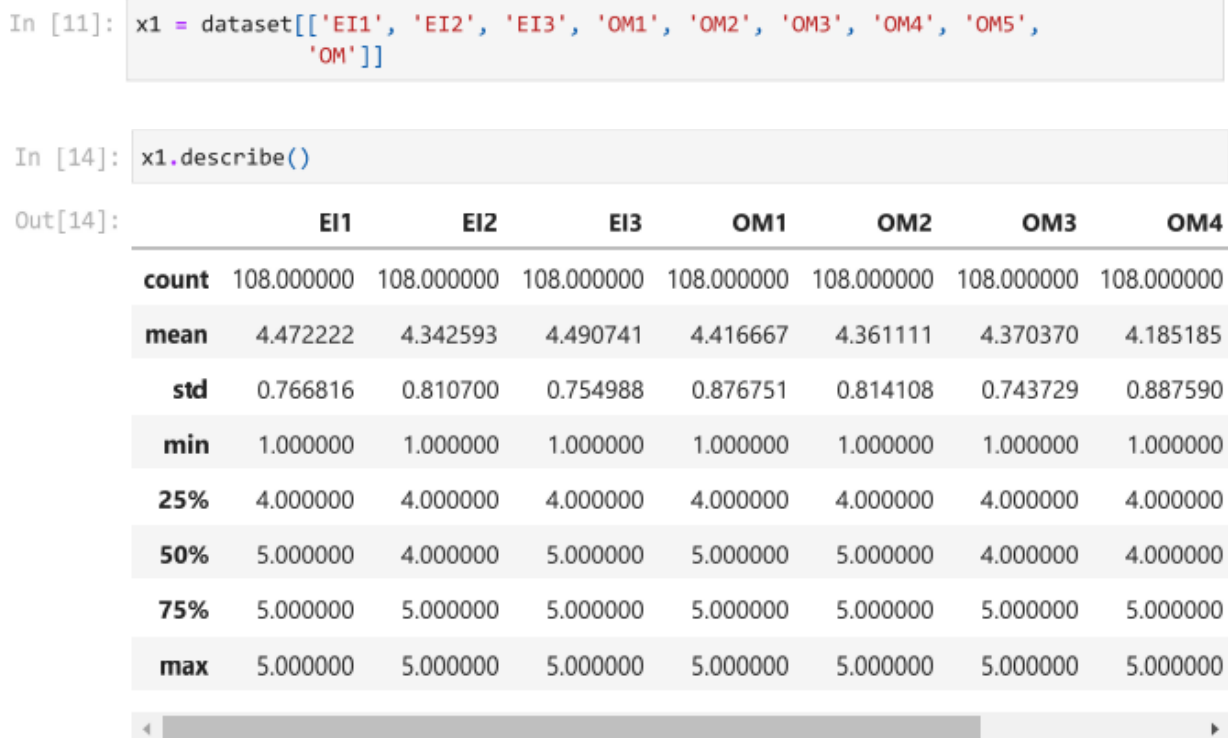


Figure 49: Values of External Influences and Organizational Mechanisms in Python

A previous figure illustrates the values imported into the system using Python for the External Influences and Organizational Mechanisms variables. Having reviewed the overall chart generated by Python and ensured each factor has been revised separately to ensure all inputs are correct and no errors have been found, the researcher has checked the values of each figure in the overall chart.

4.3.3. Feature Engineering

4.3.3.1. Correlation

An analysis of correlation measures the direction and strength of a relationship between two variables in a bivariate manner. In statistics, there are four types of correlations; Pearson, Kendall Rand, Spearman, and point-bisection. This correlation analysis is used in feature engineering to identify correlated data, removing those that are correlated. In the current research, the correlation analysis helps reduce the size of data and focuses on the smaller amount of data. Here is a graph extracted from Python showing the correlation between the data:

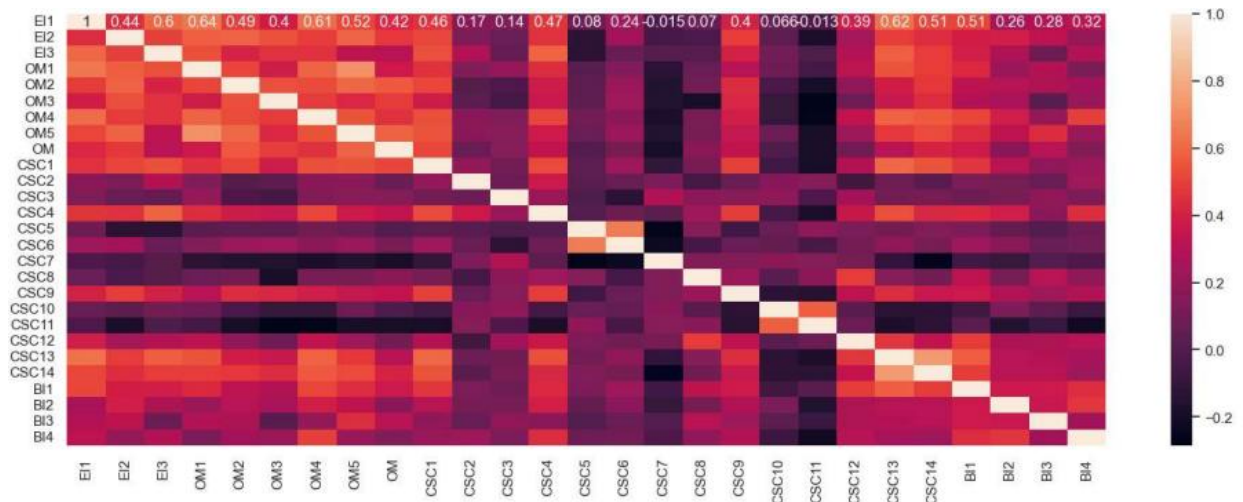


Figure 50: Pre-removal Correlation Graph

The darker the color of the data, the more correlated it is, and the darker the color, the darker the correlation. Moreover, all correlated parameters over 0.70 are removed in this research, as well as an easy and visualized method to acquire the correlation values of parameters was formulated using this graph in the machine learning pipeline. As a result of machine learning, correlated data can be automatically detected by the method, and then further instructions to remove the correlated parameters can be coded in by the researcher.

Using the correlation graph, correlated parameters and removed correlated data were compiled in the following table:

#	Parameter 1	Parameter 2	Correlation	Removed Parameter
1	EI2	EI3	0.6	CSC14
2	EI2	CSC13	0.62	
3	EI2	OM1	0.64	

Table 30: Study Parameters Correlated

Figure 51 shows the correlation between CSC13 and CSC14. CSC14 has been removed because of its high correlation with CSC13:

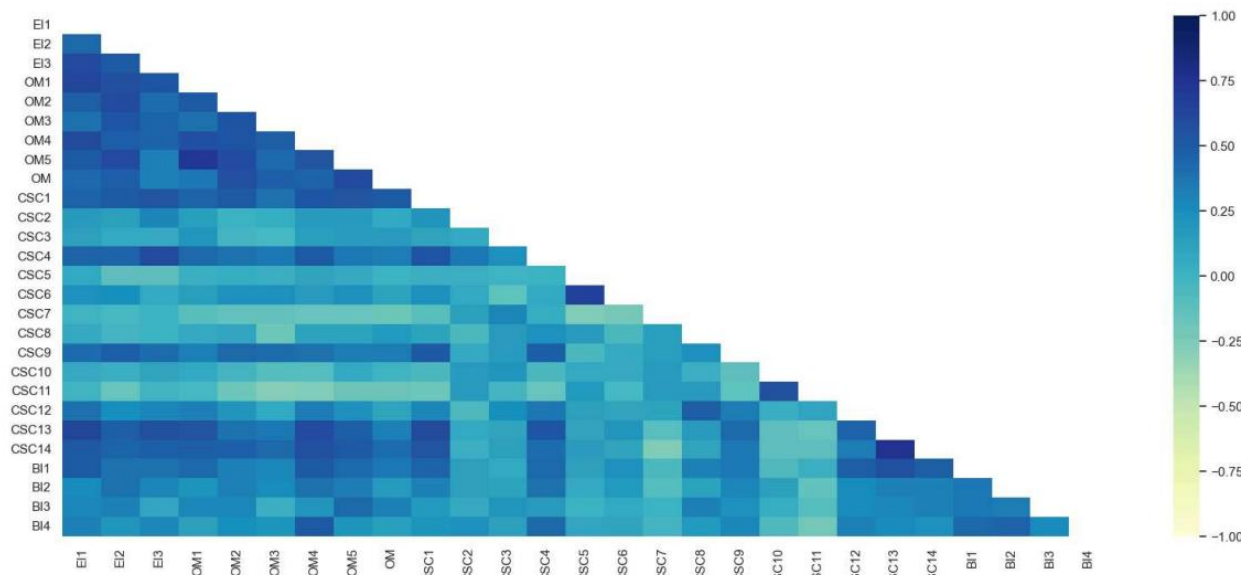


Figure 51: Variables with high correlation Graph

When implementing the SVM algorithm, the process of removing correlated data ensures that the results of the machine learning pipeline will be more accurate. The removal of correlated data is an essential step before the deployment.

4.3.3.2. Mean and Standard Deviation

A sample's mean is equal to the sum of all the responses divided by the number of responses, according to Techopedia (2019).

A comparison of Gareth, et al. (2021) explains that the Standard Deviation is the measurement of how dispersed data is within a dataset. The authors explain that when the Standard Deviation is low, it informs the researcher that the data is not dispersed as much or spread as it should, and by contrast, when the Standard Deviation is high, it indicates that the data is not disperse or spread out as much. A standard deviation above 0 in the Standard Deviation Analysis indicates that the value of the data is the same while a standard deviation below 0 means that the data value is the same.

An analysis of the information obtained during interviews is presented in the following table:

Parameter	No.	Minimum	Maximum	Mean	Standard Deviation
EI1	108	1	5	4.472222	0.766816
EI2	108	1	5	4.342593	0.810700
EI3	108	1	5	4.490741	0.754988
OM1	108	1	5	4.416667	0.876751
OM2	108	1	5	4.361111	0.814108
OM3	108	1	5	4.370370	0.743729
OM4	108	1	5	4.185185	0.887590
OM5	108	1	5	4.472222	0.662173

CSC1	108	1	5	3.342593	1.161388
CSC2	108	1	5	4.920455	1.683057
CSC3	108	1	5	3.601852	1.067268
CSC4	108	1	5	4.120370	0.828438
CSC5	108	1	5	3.203704	1.002420
CSC6	108	1	5	3.212963	0.976843
CSC7	108	1	5	3.083333	0.996489
CSC10	108	1	5	2.675926	1.206127
CSC11	108	1	5	2.277778	1.066336
CSC12	108	1	5	3.759259	1.040043
CSC13	108	1	5	4.333333	0.842781
CSC14	108	1	5	4.351852	0.878772
BI1	108	1	5	4.092593	0.859657
BI2	108	1	5	4.037037	0.796322

Table 31: Parameter Means and Standard Deviations

It is shown in the above table that the mean and standard deviation of the interview participants, as well as the mean of all parameters within the variables of external influences and organizational mechanisms, fall between the 4.1 and 4.4 range, which indicates the participants responded on average with the Likert Scale attribute of agree. However, the standard deviations of the variables fall between 0.7 and 0.8, which indicates that the distribution is relatively constant and clusters around the mean.

The following figure illustrates how the mean and standard deviation are calculated in Python:

Out[17]:

	EI1	EI2	EI3	OM1	OM2	OM3	OM4
count	108.000000	108.000000	108.000000	108.000000	108.000000	108.000000	108.000000
mean	4.472222	4.342593	4.490741	4.416667	4.361111	4.370370	4.185185
std	0.766816	0.810700	0.754988	0.876751	0.814108	0.743729	0.887590
min	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000
25%	4.000000	4.000000	4.000000	4.000000	4.000000	4.000000	4.000000
50%	5.000000	4.000000	5.000000	5.000000	5.000000	4.000000	4.000000
75%	5.000000	5.000000	5.000000	5.000000	5.000000	5.000000	5.000000
max	5.000000	5.000000	5.000000	5.000000	5.000000	5.000000	5.000000

8 rows × 27 columns

Figure 52: Parameter Means and Standard Deviations

In the following table, we show the mean of each variable (Factor) based on interviewee responses:

Factor (Variable)	Mean	Standard Deviation
External Influences	4.435185185	0.777060957
Organizational Mechanisms	4.318181818	0.810995375

Table 32: Variable Means and Standard Deviations

4.3.4. Selection of Model

Our study uses the Support Vector Machine model as our machine learning model. Statistical Learning Theory (SLT)-based Support Vector Machines (SVMs) have become increasingly popular as effective machine learning algorithms (Wang et al., 2014). The researcher selected this model because SVM learning is one of many machine learning algorithms, and compared to other ML algorithms it can detect subtle patterns in complex datasets with great accuracy.

With SVM, you can build a classifier that calculates labels based on some or all of the features within a feature vector. With SVM, you can solve problems related to pattern recognition and regression using an elegant tool for solving patterns.

The main reason for its popularity over the past few years has been its ability to provide excellent generalization performance, and it has drawn the interest of researchers in neural networks and mathematical programming. SVMs have also been demonstrated to have valuable properties in a variety of real world applications (Shevade et al., 2000).

A binary classifier is the initial form of an SVM, in which either a positive or a negative output is obtained from the learned function. A SVM is normally used to learn classification, regression, or ranking functions. (Yu & Kim, 2012) Classifying SVMs, support vector regression systems (SVRs), and ranking SVMs (or RankSVMs) are all called classifying SVMs.

Generally, SVMs are classified into two types: linear SVMs and quadratic SVMs based on their empirical error in classification and geometric boundary.

Due to the remarkable effect it produces, SVM has been extensively advocated by researchers in a variety of domains. As a result of its ability to handle multidimensional information and complex feature issues, SVM plays a vital role in the development of artificial intelligence. Furthermore, it is capable of integrating the theory of statistical learning with categorization of internal maximization. The robustness of SVM in narrow sample sizes makes it superior to other predictive procedures and allows it to correct the local peak fault (Ali et al., 2024).

Despite the SVM's good performance in cybersecurity, its kernel functions must be selected, constructed and improved to improve its performance (Dasgupta et al., 2020).

Ali et al., (2024) conducted a research about Efficient Cybersecurity Assessment Using SVM and Fuzzy Evidential Reasoning for Resilient Infrastructure and founded from their results that SVM has a slightly better accuracy than other applied models of machine learning.

Prior to the final selection of the model, the data were trained and tested on a subset of the data to select the model, as well. Finally, and in summary, SVM is the recommended machine learning model.

4.3.5. Training the Model

For the efficient, effective use of SVMs, an important aspect is the training algorithm, for which, several authors have developed methods such as the hyper parameter selection method (Martinez Torres et al., 2019).

Training data are used to impose a test set on the model, and calculation errors are applied to the inputs for training or testing in order to adjust the model or train it more accurately. It is essential that the model is ready to distinguish between attacker and normal node when it has been designed and accurately reached based on input training and testing. Otherwise, the design process needs to be corrected (Kajal & Nandal, 2020).

Using the sklearn library in Python, a SVM classifier can be developed automatically (Komer et al., 2014). Sklearn is a new software project that provides automatic algorithm configuration for the Scikit-learn machine learning library. One of the key objectives of Sklearn is its ease of use and learning (Bergstra et al., 2015).

An Anaconda distribution of Python and R software for scientific computing has been installed by the researcher, which simplifies package management and deployment for these languages. In the next step, the researcher will use a code

saved under this study, this code will only be accessible by the researcher and not by anyone else. A machine learning pipeline is used to train the model using the excel sheet that contains the interviewees answers. We verify that all questions have been answered and delete the blank fields that have not been answered. The following figure illustrates the code that was used during the training process:

Following this, we classified the X and Y variables into independent and dependent variables respectively, since X contains the inputs, while Y contains the outputs, which are the dependent variables.

```
In [9]: dataset.columns

Out[9]: Index(['Gender', 'Age', 'Marital Status', 'Education Level', 'Field of study',
              'Your job Title', 'IT Security Certifications', 'Work Experience',
              'Number of employees', 'IT department number of employees', 'EI1',
              'EI2', 'EI3', 'OM1', 'OM2', 'OM3', 'OM4', 'OM5', 'OM', 'CSC1', 'CSC2',
              'CSC3', 'CSC4', 'CSC5', 'CSC6', 'CSC7', 'CSC8', 'CSC9', 'CSC10',
              'CSC11', 'CSC12', 'CSC13', 'CSC14', 'BI1', 'BI2', 'BI3', 'BI4', 'CSB1',
              'CSB2', 'CSB3', 'CSB4', 'CSB5', 'Unnamed: 42'],
              dtype='object')
```

Figure 53: The import of datasets in machine learning

As a next step, the researcher divided the dataset into training and testing sets in Python, estimating the performance of machine learning algorithms suited for predictive algorithms or applications by using the train-test split. We can compare our own machine learning model results to those from the machine using this method, which is fast and easy to do.

```

In [10]: X = dataset[['EI1', 'EI2', 'EI3', 'OM1', 'OM2', 'OM3', 'OM4', 'OM5',
                    'OM', 'CSC1', 'CSC2', 'CSC3', 'CSC4', 'CSC5', 'CSC6', 'CSC7',
                    'CSC8', 'CSC9', 'CSC10', 'CSC11', 'CSC12', 'CSC13',
                    'CSC14', 'BI1', 'BI2', 'BI3', 'BI4',]]
y = dataset[['CSB1']]

In [11]: x1 = dataset[['EI1', 'EI2', 'EI3', 'OM1', 'OM2', 'OM3', 'OM4', 'OM5',
                    'OM']]

In [12]: x2 = dataset[['CSC1', 'CSC2', 'CSC3', 'CSC4', 'CSC5', 'CSC6', 'CSC7',
                    'CSC8', 'CSC9']]

In [13]: x3 = dataset[['CSC10', 'CSC11', 'CSC12', 'CSC13', 'CSC14',
                    'BI1', 'BI2', 'BI3', 'BI4',]]

In [14]: x1.describe()

```

Figure 54: Python code for splitting a dataset into Train and Test Sets

By using kernel as the linear kernel in SVC() function, the researcher has constructed a support vector machine model, imported the SVM module, and created a support vector classifier object.

```

In [29]: from sklearn import svm, datasets
import sklearn.model_selection as model_selection
from sklearn.metrics import accuracy_score
from sklearn.metrics import f1_score

```

Figure 55: SVM classifier model initialization

To predict the test set, the researcher fits the model using fit () on the train set and performs the prediction using predict

```

In [30]: from sklearn.model_selection import train_test_split
X_train,X_test,y_train,y_test = train_test_split(X,y,test_size=0.3,random_state=42)

In [31]: rbf = svm.SVC(kernel='rbf', gamma=0.5, C=0.1).fit(X_train, y_train)
poly = svm.SVC(kernel='poly', degree=3, C=1).fit(X_train, y_train)

```

Figure 56: Model fitting with SVM

```

In [32]: poly_pred = poly.predict(X_test)
rbf_pred = rbf.predict(X_test)

```

Figure 57: Making predictions

To determine the accuracy of the SVM model after training, the researcher compares the actual values of the test set with the predictions.

```
In [33]: poly_accuracy = accuracy_score(y_test, poly_pred)
poly_f1 = f1_score(y_test, poly_pred, average='weighted')
print('Accuracy (Polynomial Kernel): ', "%.2f" % (poly_accuracy*100))
print('F1 (Polynomial Kernel): ', "%.2f" % (poly_f1*100))

Accuracy (Polynomial Kernel):  69.70
F1 (Polynomial Kernel):  69.34

In [34]: rbf_accuracy = accuracy_score(y_test, rbf_pred)
rbf_f1 = f1_score(y_test, rbf_pred, average='weighted')
print('Accuracy (RBF Kernel): ', "%.2f" % (rbf_accuracy*100))
print('F1 (RBF Kernel): ', "%.2f" % (rbf_f1*100))

Accuracy (RBF Kernel):  54.55
F1 (RBF Kernel):  38.50
```

Figure 58: Performance evaluation of the model

We will discuss in the following section how the model evaluation impacts the accuracy of the study.

4.3.6. Model Evaluation

As part of the machine learning pipeline, it is crucial to evaluate the model after it has been trained and tested thoroughly using stratified sampling.

To evaluate the performance of a classification method, a confusion matrix is used in current research. A confusion matrix is used to identify a model's accuracy. This is a visualized approach, which provides a summary of algorithm classification performance, as described by Kulkarni, et al. (2020).

This graph illustrates how confusion matrix work, taken from Draelos (2019):

Confusion Matrix

	Actually Positive (1)	Actually Negative (0)
Predicted Positive (1)	True Positives (TPs)	False Positives (FPs)
Predicted Negative (0)	False Negatives (FNs)	True Negatives (TNs)

Figure 59: An example of a confusion matrix

Ground-truth labels refer to Actually Positive (1) and Actually Negative (0).

It refers to the model's prediction of Positive (1) and Negative (0).

In figure 61, we can see the entries in the confusion matrix (TPs, FPs, FNs, TNs) that have the following meanings:

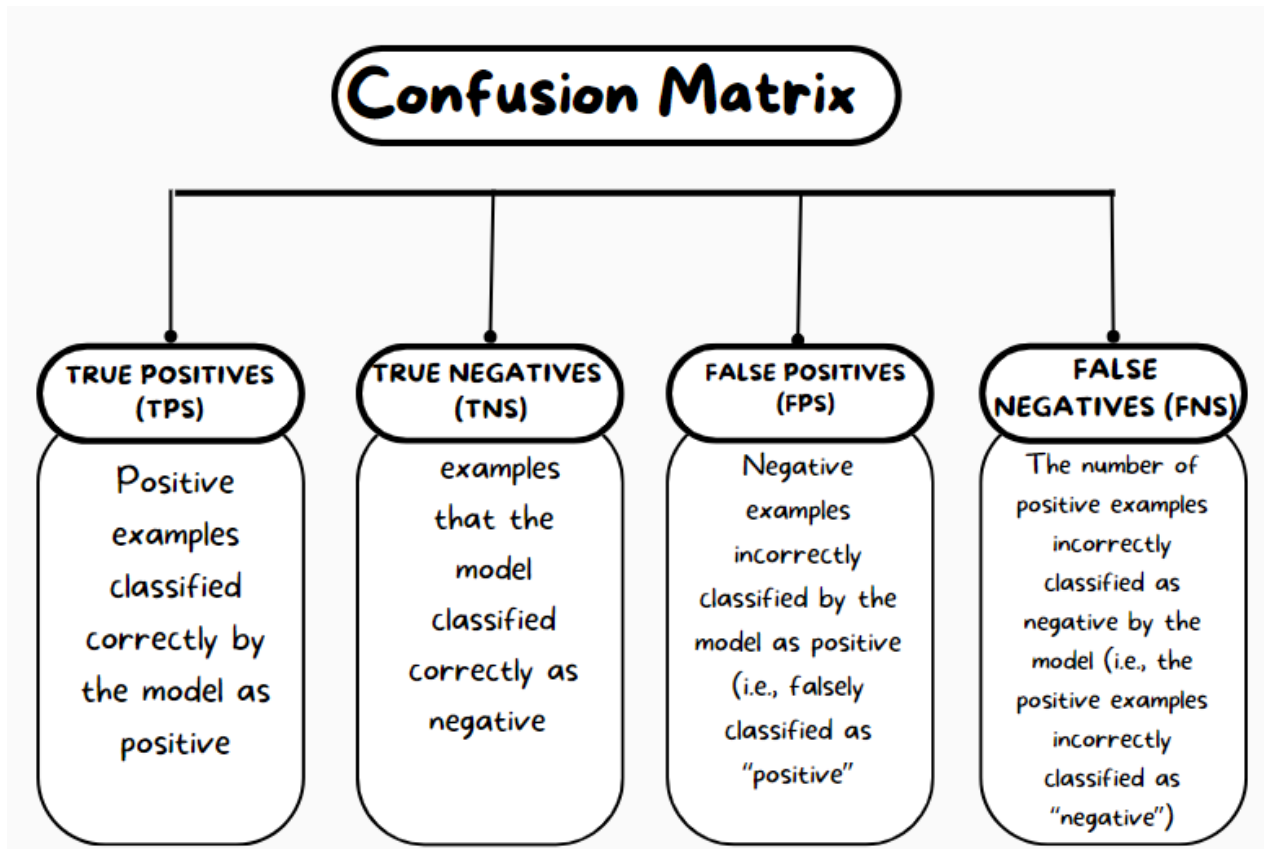


Figure 60: The entries of the confusion matrix

Draelos (2019) argues that this method can be applied to multiple models for comparing them, and all strengths and weaknesses can be quickly identified, thus making it easier to review the adopted model for machine learning. The researcher can then select the model most appropriate for research by applying this method to multiple models.

According to the confusion matrix for this study, the following results are shown:

	precision	recall	f1-score	support
3	0.67	0.50	0.57	4
4	0.70	0.78	0.74	18
5	0.70	0.64	0.67	11
accuracy			0.70	33
macro avg	0.69	0.64	0.66	33
weighted avg	0.70	0.70	0.69	33

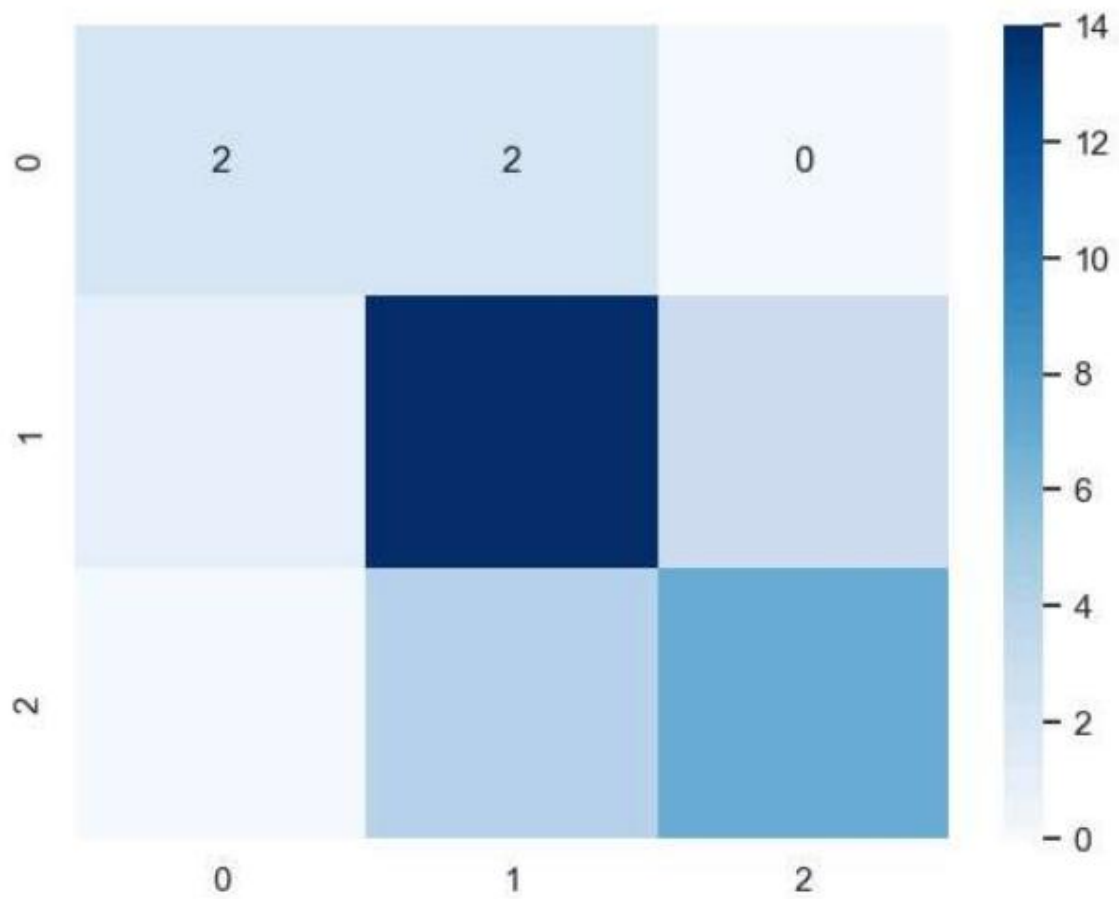


Figure 61: Study Confusion Matrix

Considering the confusion matrix from the previous figure, there are 4 correct positive examples in the model and 0 incorrect negative examples, making a total of 4 correct positive examples. The model incorrectly classified 0 negative

examples as positive, and 0 negative examples as negative, making a total of 0 examples incorrectly classified as negative by the model.

It appears that the SVC Classifier model passed evaluation and can be used to analyze the results of this study, since the accuracy rate is 0.70, which means that 70% of the findings can be accurate.

4.3.7. Result and Discussion

We discuss the findings in this section, and graphs and illustrations are generated by using the SVM algorithm through the machine learning pipeline. This section gives a comprehensive explanation of cybersecurity culture, explains the results of the figure table, and discusses the factors associated with cybersecurity culture.

A discussion of the hypothesis follows in each part, which presents an overview of the parameters extracted from Python and their acronyms based on their definition in Python, followed by an analysis of the parameter rankings (parameter rankings) based on the significance measure from SVM. This paper provides a detailed explanation of the ranking within each factor as well as a discussion of the hypotheses of each variable. Finally, the recommended equation is actually implemented in this paper so that interested future users can follow the same process to ultimately measure their cybersecurity behavior.

4.3.7.1. Parameters Importance

With the SVM algorithm, the importance of parameters was identified by the following codes:

```
from sklearn.ensemble import ExtraTreesClassifier
model = ExtraTreesClassifier()
model.fit(X,y)
```

```
feat_importances = pd.Series(model.feature_importances_,index =X.columns)
feat_importances.nlargest(27).plot(kind="barh")
plt.show()
```

Figure 62: SVM Code of Parameter Importance

To begin with, we should show how parameters (features) look in SVM:

```
print(model.feature_importances_)
[0.04206775 0.03349641 0.02823149 0.02428111 0.02924882 0.02009018
 0.07821362 0.0249563  0.03062041 0.05486563 0.02847488 0.03732893
 0.033732   0.03844546 0.02691244 0.02328174 0.02581082 0.02174798
 0.02740627 0.03811836 0.06176844 0.06597537 0.06276013 0.04921986
 0.0929456 ]
```

Figure 63: Scores computed by SVM

Below are two tables that present a detailed description of the previously extracted data from SVM, the first table presents the Features Scores, while the second table presents the Features Ranking. The tables provide a detailed explanation of the Parameters (Features).

Table 1: Detailed Feature Scores

Feature scores are presented in the following table, filtered by parameter codes:

Parameter	Feature Number	Importance Measure	Rank	Factor	Sub factor
EI1	Feature: 0	0.04206775	Rank 8	External Influences	Societal Cybersecurity Culture
EI2	Feature: 1	0.03349641	Rank 13	External Influences	External Rules and Regulations
EI3	Feature: 2	0.02823149	Rank 17	External Influences	Peer Institutions

OM1	Feature: 3	0.02428111	Rank 22	Organizational Mechanisms	Cybersecurity Culture Leadership
OM2	Feature: 4	0.02924882	Rank 15	Organizational Mechanisms	Performance Evaluations
OM3	Feature: 5	0.02009018	Rank 25	Organizational Mechanisms	Rewards and Punishments
OM4	Feature: 6	0.07821362	Rank 2	Organizational Mechanisms	Organizational Learning
OM5	Feature: 7	0.0249563	Rank 21	Organizational Mechanisms	Cybersecurity Training
OM6	Removed Feature			Organizational Mechanisms	Communications Channel
OM7	Removed Feature			Organizational Mechanisms	Budget
CSC1	Feature: 8	0.03062041	Rank 14	Cybersecurity Culture	Inter-department Collaboration
CSC2	Feature: 9	0.05486563	Rank 6	Cybersecurity Culture	Community Norms and Beliefs
CSC3	Feature: 10	0.02847488	Rank 16	Cybersecurity Culture	Top Management's Priorities
CSC4	Feature: 11	0.03732893	Rank 11	Cybersecurity Culture	Top Management's Participation

CSC5	Feature: 12	0.033732	Rank 12	Cybersecurity Culture	Top Management's Participation
CSC6	Feature: 13	0.03844546	Rank 9	Cybersecurity Culture	Top Management's knowledge
CSC7	Feature: 14	0.02691244	Rank 19	Cybersecurity Culture	Top Management's Priorities
CSC8	Feature: 15	0.02328174	Rank 23	Cybersecurity Culture	Top Management's Participation
CSC9	Feature: 16	0.02581082	Rank 20	Cybersecurity Culture	Teamwork Perception
CSC10	Feature: 17	0.02174798	Rank 24	Cybersecurity Culture	General Cyber Threat Awareness
CSC11	Feature: 18	0.02740627	Rank 18	Cybersecurity Culture	General Cyber Threat Awareness
CSC12	Feature: 19	0.03811836	Rank 10	Cybersecurity Culture	Employee's Self-Efficacy
CSC13	Feature: 20	0.06176844	Rank 5	Cybersecurity Culture	Cybersecurity Policy Awareness

CSC14	Removed Feature			Cybersecurity Culture	Cybersecurity Policy Awareness
BI1	Feature: 21	0.06597537	Rank 3	Behavior Intention	Cybersecurity Training and Intention
BI2	Feature: 22	0.06276013	Rank 4	Behavior Intention	Cybersecurity Policy and Intention
BI3	Feature: 23	0.04921986	Rank 7	Behavior Intention	External Cybersecurity
BI4	Feature: 14	0.0929456	Rank 1	Behavior Intention	Cybersecurity culture and intention

Table 32: Detailed Feature Scores

In the correlation testing of the machine learning pipeline, three parameters were eliminated before the SVM algorithm was initiated. Therefore, the parameters OM6, OM7 and CSC 14 are no longer included in the SVM features. Here is a graph illustrating the previous table visually using Microsoft Excel:

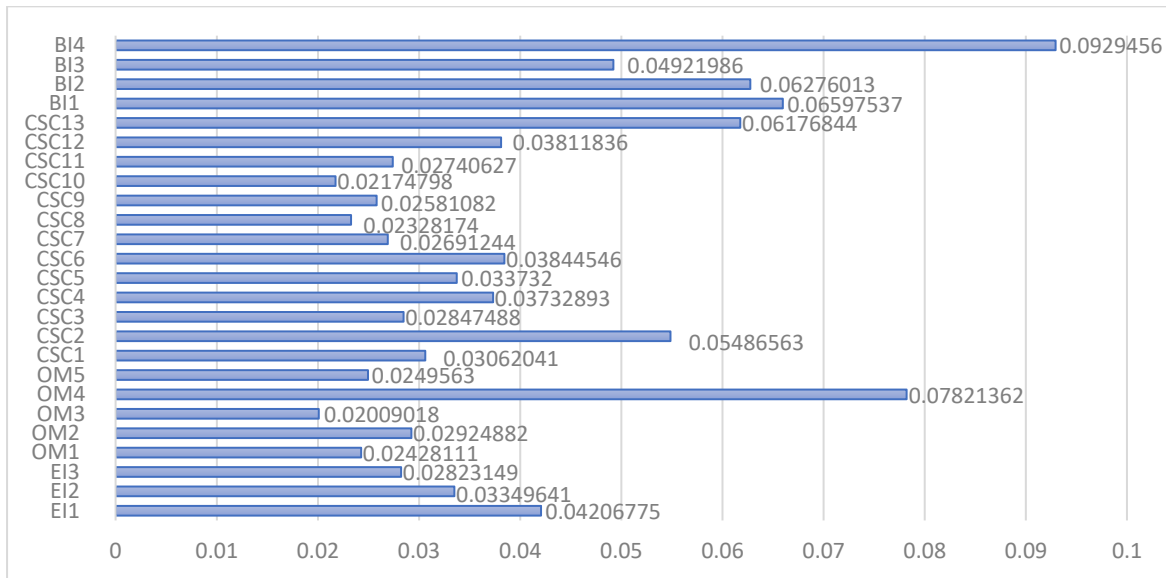


Figure 64: Features scored in detail

Table 2: Detailed Feature Ranking

According to the importance measure, the following table represents the feature ranking:

Rank	Importance Measure	Parameter	Feature Number	Factor	Sub factor
Rank 1	0.0929456	BI4	Feature: 14	Behavior Intention	Cybersecurity culture and intention
Rank 2	0.07821362	OM4	Feature: 6	Organizational Mechanisms	Organizational Learning
Rank 3	0.06597537	BI1	Feature: 21	Behavior Intention	Cybersecurity Training and Intention

Rank 4	0.06276013	BI2	Feature: 22	Behavior Intention	Cybersecurity Policy and Intention
Rank 5	0.06176844	CSC13	Feature: 20	Cybersecurity Culture	Cybersecurity Policy Awareness
Rank 6	0.05486563	CSC2	Feature: 9	Cybersecurity Culture	Community Norms and Beliefs
Rank 7	0.04921986	BI3	Feature: 23	Behavior Intention	External Cybersecurity
Rank 8	0.04206775	EI1	Feature: 0	External Influences	Societal Cybersecurity Culture
Rank 9	0.03844546	CSC6	Feature: 13	Cybersecurity Culture	Top Management's knowledge
Rank 10	0.03811836	CSC12	Feature: 19	Cybersecurity Culture	Top Management's knowledge
Rank 11	0.03732893	CSC4	Feature: 11	Cybersecurity Culture	Top Management's Participation
Rank 12	0.033732	CSC5	Feature: 12	Cybersecurity Culture	Top Management's Participation

Rank 13	0.03349641	EI2	Feature: 1	External Influences	External Rules and Regulations
Rank 14	0.03062041	CSC1	Feature: 8	Cybersecurity Culture	Inter-department Collaboration
Rank 15	0.02924882	OM2	Feature: 4	Organizational Mechanisms	Performance Evaluations
Rank 16	0.02847488	CSC3	Feature: 10	Cybersecurity Culture	Top Management's Priorities
Rank 17	0.02823149	EI3	Feature: 2	External Influences	Peer Institutions
Rank 18	0.02740627	CSC11	Feature: 18	Cybersecurity Culture	General Cyber Threat Awareness
Rank 19	0.02691244	CSC7	Feature: 14	Cybersecurity Culture	Top Management's Priorities
Rank 20	0.02581082	CSC9	Feature: 16	Cybersecurity Culture	Teamwork Perception
Rank 21	0.0249563	OM5	Feature: 7	Organizational Mechanisms	Cybersecurity Training
Rank 22	0.02428111	OM1	Feature: 3	Organizational Mechanisms	Cybersecurity Culture Leadership
Rank 23	0.02328174	CSC8	Feature: 15	Cybersecurity Culture	Top Management's Participation

Rank 24	0.02174798	CSC10	Feature: 17	Cybersecurity Culture	General Cyber Threat Awareness
Rank 25	0.02009018	OM3	Feature: 5	Organizational Mechanisms	Rewards and Punishments
Removed Feature		OM6	-	Organizational Mechanisms	Communications Channel
Removed Feature		OM7	-	Organizational Mechanisms	Budget
Removed Feature		CSC14	-	Cybersecurity Culture	Cybersecurity Policy Awareness

Table 33: Detailed Feature Ranking

Below you will find a graph that illustrates the previous table visually using Microsoft Excel, followed by a graph produced using Python to illustrate the ranking of the features:

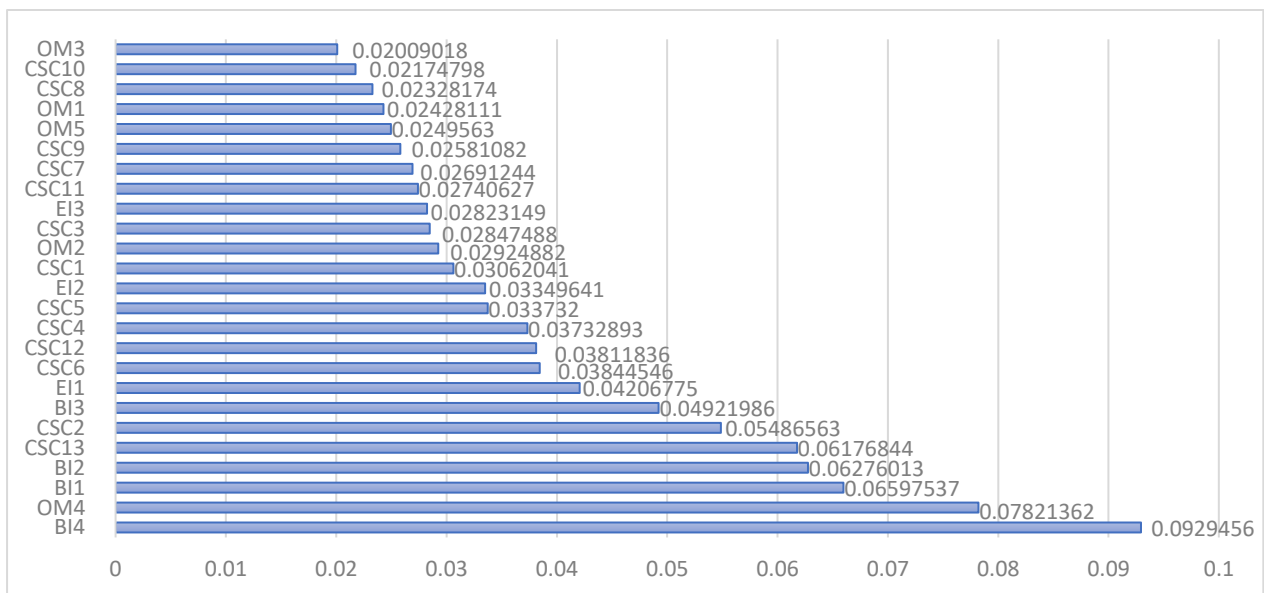


Figure 65: Rankings by feature detail

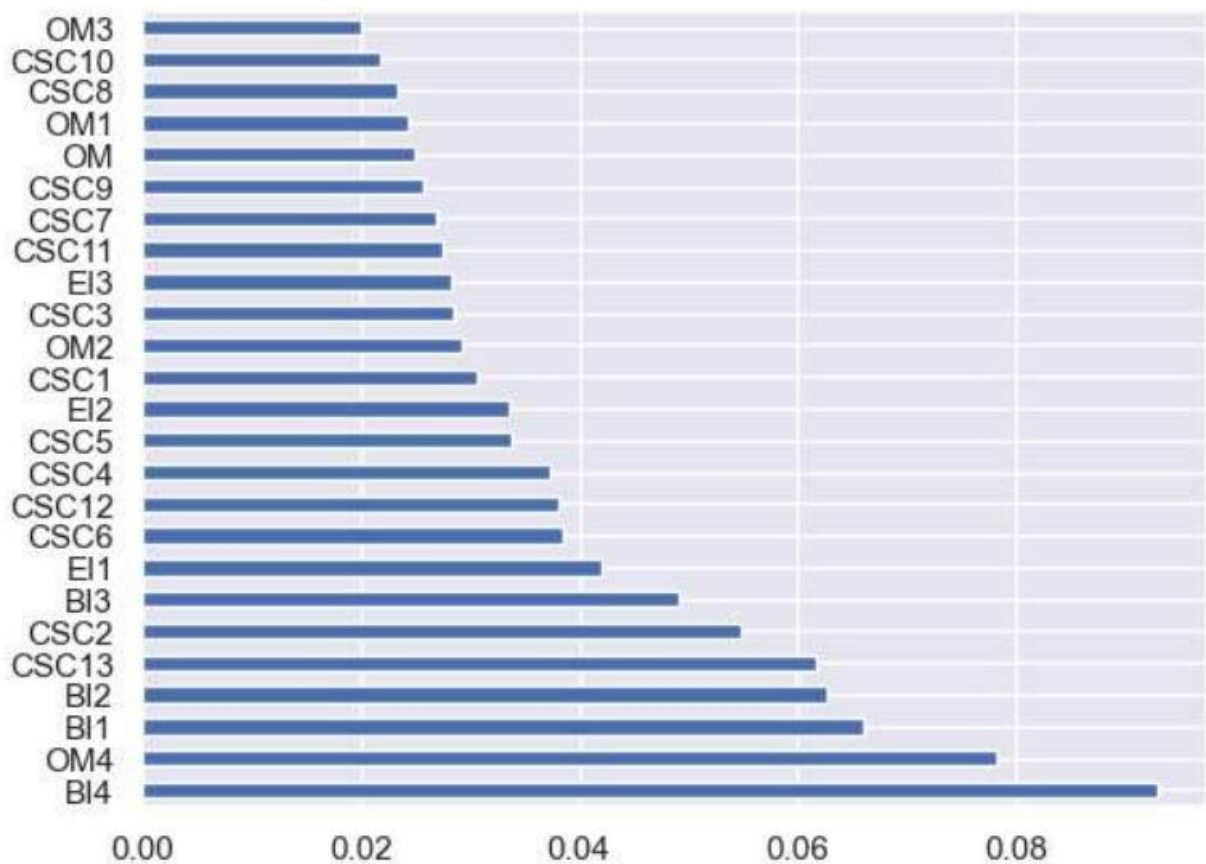


Figure 66: An extract of the Python feature ranking graph

Discussion of Top Parameters:

Organizational Mechanisms (OM), Organizational Learning sub factor (OM4) with 0.07821362 importance measure is the number one ranking obtained from SVM and SVC classifiers. Hence, the most important parameter contributing to adopting cybersecurity is the learning process of the employees within the organization, starting with the board of directors and ending with the smallest employee. These are things like building skills, sharing information, or adding new insights to the organization about cybersecurity.

As the second most important sub factor of the external influences factors (EI), the Societal Cybersecurity Culture sub factor (EI1) is found to affect the cybersecurity culture as much as the second most important parameter. Based on the importance measure of 0.04206775, Bahrain is paying an excellent deal of attention to the level of cyber security, which is why banks are benefited by such features.

In third rank, the External Rules and Regulations (EI2) of the External Influences (EI) were found to be the third most important parameter entails whether affects bank cybersecurity culture, with an importance level of 0.03349641, meaning that government and central bank rules and regulations are highly influential factors that impact bank cybersecurity culture. Government regulations should ensure that banks' rights are protected.

The fourth most important parameter that affects the cybersecurity culture of the bank is the Performance Evaluation sub factor (OM2) of the organizational mechanism factors (OM). It has an importance measure of 0.02944882, the fourth most important parameter. In short and long term, regular performance evaluations incurred by management will have an impact on the banks' cybersecurity culture because they help the management evaluate the weaknesses and strengths of employees.

As a ranking indicator in fifth rank, Peer Institutions find that external influences (EI) are important to cybersecurity culture in the banks, and it has an important value of 0.02823149. As a result, if the peer banks have improved their cybersecurity levels, then the bank will also be better in this area, whereas the opposite is true as well.

Last but not least, the organizational mechanisms (OM) are ranked at the sixth, seventh, and eighth levels. This includes Cybersecurity Training (OM5), which ranks sixth with 0.0249563 importance, Cybersecurity Culture Leadership (OM1), which ranks seventh with 0.02428111 importance, and Rewards and Punishments (OM3), which ranks eighth and is 0.02009018 in importance. All of these internal factors have an impact on cybersecurity culture.\

4.3.7.2. External Influences

In this part of the paper, we'll discuss the parameters within External Influences (Variables), starting with a table that shows the parameters and their rankings, as well as their ranking score and their Python feature number.

Rank	Importance Measure	Parameter	Feature Number	Factor	Sub factor
Rank 8	0.04206775	EI1	Feature: 0	External Influences	Societal Cybersecurity Culture

Rank 13	0.03349641	EI2	Feature: 1	External Influences	External Rules and Regulations
Rank 17	0.02823149	EI3	Feature: 2	External Influences	Peer Institutions

Table 34: Ranking Scores based on external influences

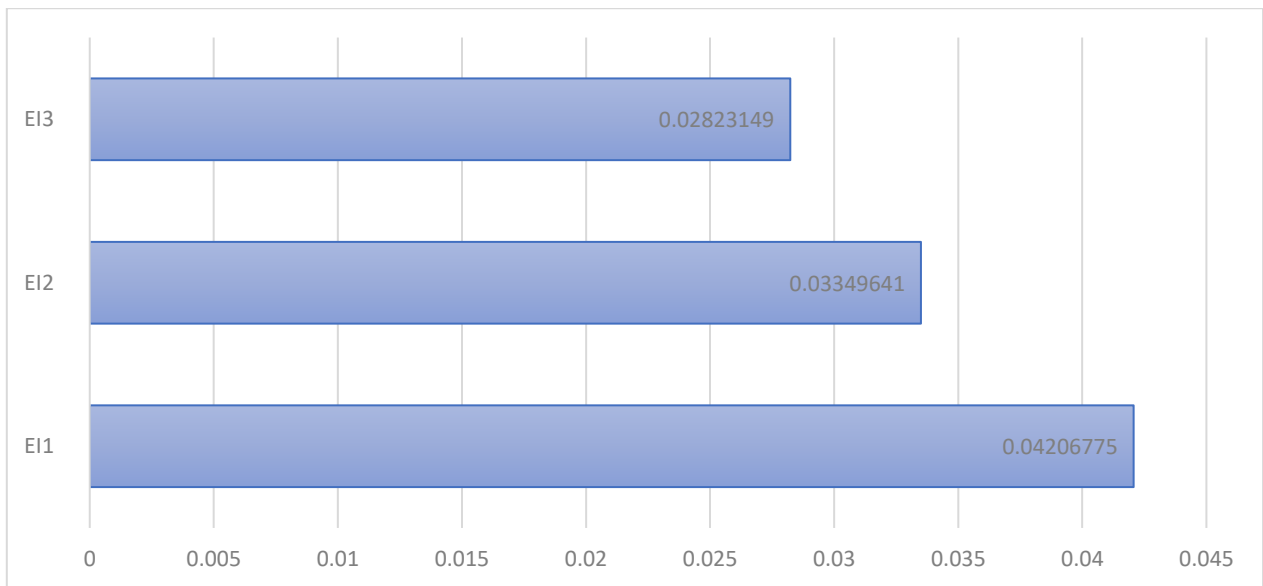


Figure 67: Ranking Scores based on external influences

Among the External Influences, Table 2 and Figure 3 show that Societal Cybersecurity Culture (EI1) has the highest ranking score with an importance measure of 0.04206775%.

4.3.7.3. Organizational Mechanisms

We will begin with displaying the table with the parameters and their ranking, as well as their ranking score and their feature number abbreviated by Python. Within the section we will present the parameters (Sub factors) within the Organizational Mechanisms Factors (OM) variable.

Rank	Importance Measure	Parameter	Feature Number	Factor	Sub factor
------	--------------------	-----------	----------------	--------	------------

Rank 22	0.02428111	OM1	Feature: 3	Organizational Mechanisms	Cybersecurity Culture Leadership
Rank 15	0.02924882	OM2	Feature: 4	Organizational Mechanisms	Performance Evaluations
Rank 25	0.02009018	OM3	Feature: 5	Organizational Mechanisms	Rewards and Punishments
Rank 2	0.07821362	OM4	Feature: 6	Organizational Mechanisms	Organizational Learning
Rank 21	0.0249563	OM5	Feature: 7	Organizational Mechanisms	Cybersecurity Training

Table 35: Ranking Scores based on Organizational Mechanisms

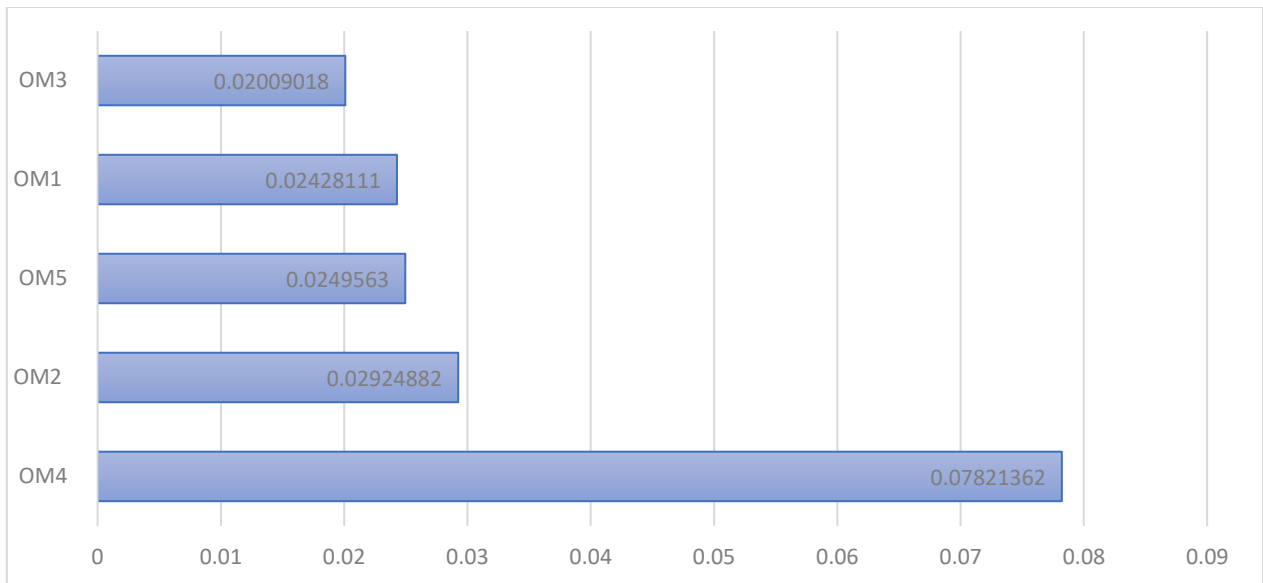


Figure 68: Ranking Scores based on Organizational Mechanisms

Based on the figures and table above, it can be seen that the organizational learning (OM4) Sub factor is more influential on cybersecurity culture than the performance evaluation sub factor (OM2). In addition to being the top-ranked factor in External Influences Factors, it also ranks as the second-most important parameter overall.

4.3.7.4. Overall Factors Importance Measure

As an important point, it is important to note that after determining the importance of each parameter, the average value of the importance measure is calculated for each factor, which means that each sub factor belongs to a particular factor was combined, and a mean measure of each factor is calculated. As a summary of the Factor Importance Measure, the table below shows the results

Rank	Factor / Variable	Importance Measure
Rank 1	Organizational Mechanisms (OM)	0.035358
Rank 2	External Influences (EI)	0.0345986

Table 36: Factors Importance Measure and Ranking

According to the table above, Organizational Mechanisms are considered the most important factor influencing cybersecurity culture. External influences rank second in importance, with the importance of organizational mechanisms very close to each other, except that organizational mechanisms rank highest.

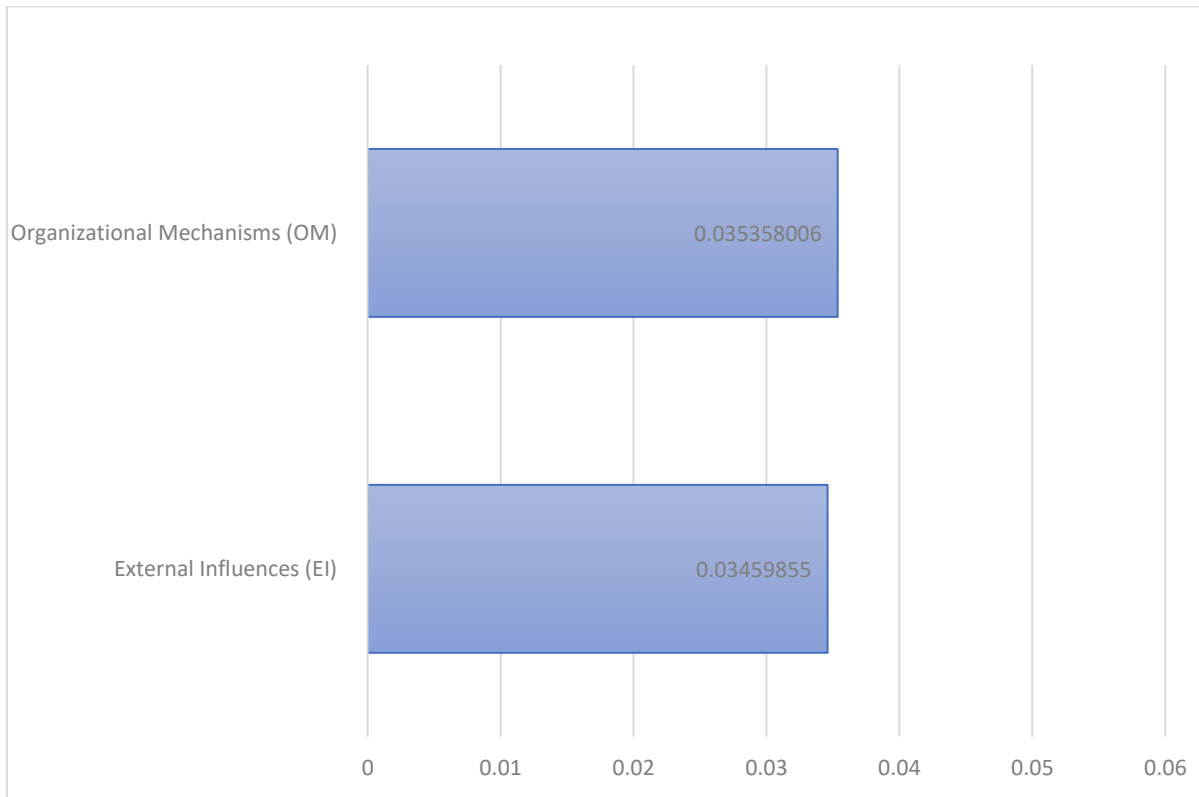


Figure 69: Factors Importance Measure and Ranking

4.3.7.5. Cybersecurity Culture

Here, we discuss the parameters within cybersecurity culture (Moderator), along with ranking scores, Python feature numbers, and ranking scores, along with a table showing the parameters and their rankings

Rank	Importance Measure	Parameter	Feature Number	Factor	Sub factor
Rank 5	0.06176844	CSC13	Feature: 20	Cybersecurity Culture	Cybersecurity Policy Awareness
Rank 6	0.05486563	CSC2	Feature: 9	Cybersecurity Culture	Community Norms and Beliefs

Rank 9	0.03844546	CSC6	Feature: 13	Cybersecurity Culture	Top Management's knowledge
Rank 10	0.03811836	CSC12	Feature: 19	Cybersecurity Culture	Top Management's knowledge
Rank 11	0.03732893	CSC4	Feature: 11	Cybersecurity Culture	Top Management's Participation
Rank 12	0.033732	CSC5	Feature: 12	Cybersecurity Culture	Top Management's Participation
Rank 14	0.03062041	CSC1	Feature: 8	Cybersecurity Culture	Inter-department Collaboration
Rank 16	0.02847488	CSC3	Feature: 10	Cybersecurity Culture	Top Management's Priorities
Rank 18	0.02740627	CSC11	Feature: 18	Cybersecurity Culture	General Cyber Threat Awareness
Rank 19	0.02691244	CSC7	Feature: 14	Cybersecurity Culture	Top Management's Priorities
Rank 20	0.02581082	CSC9	Feature: 16	Cybersecurity Culture	Teamwork Perception

Rank 23	0.02328174	CSC8	Feature: 15	Cybersecurity Culture	Top Management's Participation
Rank 24	0.02174798	CSC10	Feature: 17	Cybersecurity Culture	General Cyber Threat Awareness

Table 37: Ranking Scores based on Cybersecurity Culture

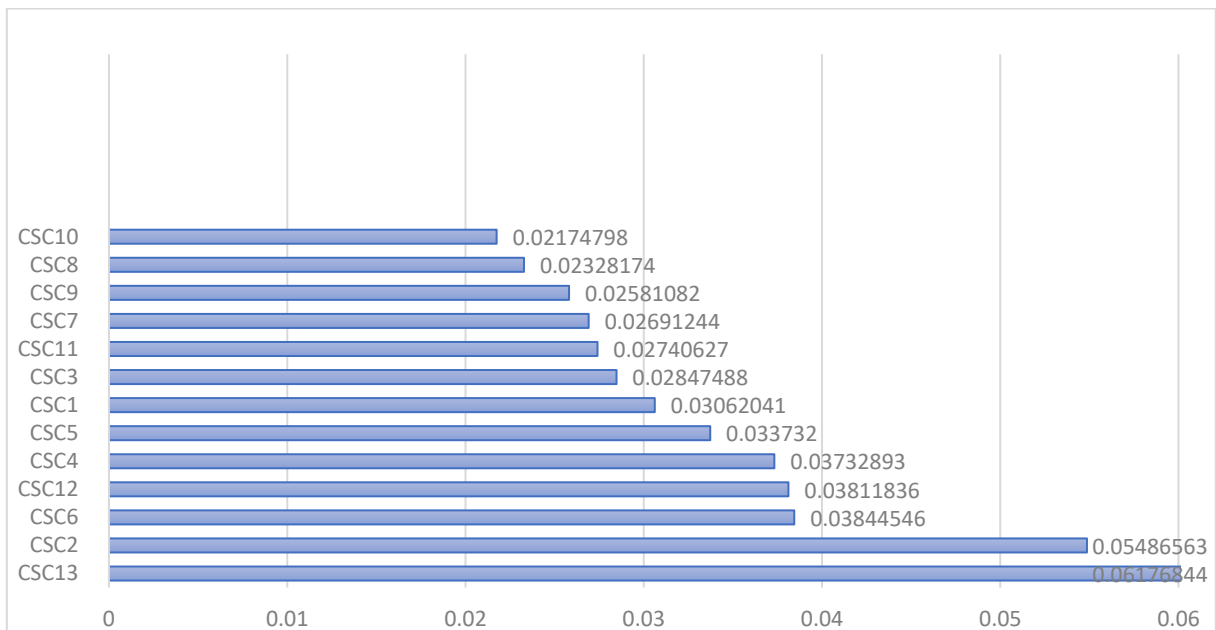


Figure 71: Ranking Scores based on Cybersecurity Culture

In light of the figures and table above, it can be seen that under the moderator of cybersecurity culture, CSC13 has the greatest importance, which is associated with cyber security policy awareness, and CSC10 is associated with general cyber threat awareness, which has the least importance.

4.3.7.6. Behavior Intention

A table showing the parameters and their ranking is included in this section, along with ranking scores, Python feature numbers, and ranking scores, as well as a discussion of Behavior Intention (Dependent Variable).

Rank	Importance Measure	Parameter	Feature Number	Factor	Sub factor
Rank 1	0.0929456	BI4	Feature: 14	Behavior Intention	Cybersecurity culture and intention
Rank 3	0.06597537	BI1	Feature: 21	Behavior Intention	Cybersecurity Training and Intention
Rank 4	0.06276013	BI2	Feature: 22	Behavior Intention	Cybersecurity Policy and Intention
Rank 7	0.04921986	BI3	Feature: 23	Behavior Intention	External Cybersecurity

Table 38: Ranking Scores based on Behavior Intention

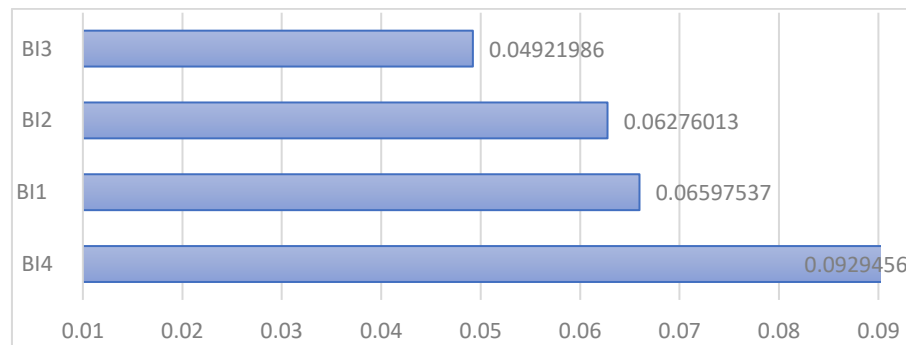


Figure 72: Ranking Scores based on Behavior Intention

Considering the above table and figure, it is evident that the behavior intention sub factor (BI4) has the highest importance measure, which is related to the importance of the bank's cybersecurity culture on employee behavior, whereas the least important ranking is associated with (BI3), which is associated with employee intention to encourage cybersecurity for others.

4.3.7.6. Cybersecurity Behavior

As one of the research objectives was to identify cybersecurity training in the banking sector, researchers have selected one sub factor for the Dependent variable, CSB1, which relates to how employees behave after receiving cyber security training. As shown in the above figure, employees are extremely likely to agree or strongly agree that the cybersecurity training provided by the banks improves their behavior.

```
In [21]: sns.set()  
sns.distplot(dataset["CSB1"],bins=10)  
plt.show()
```

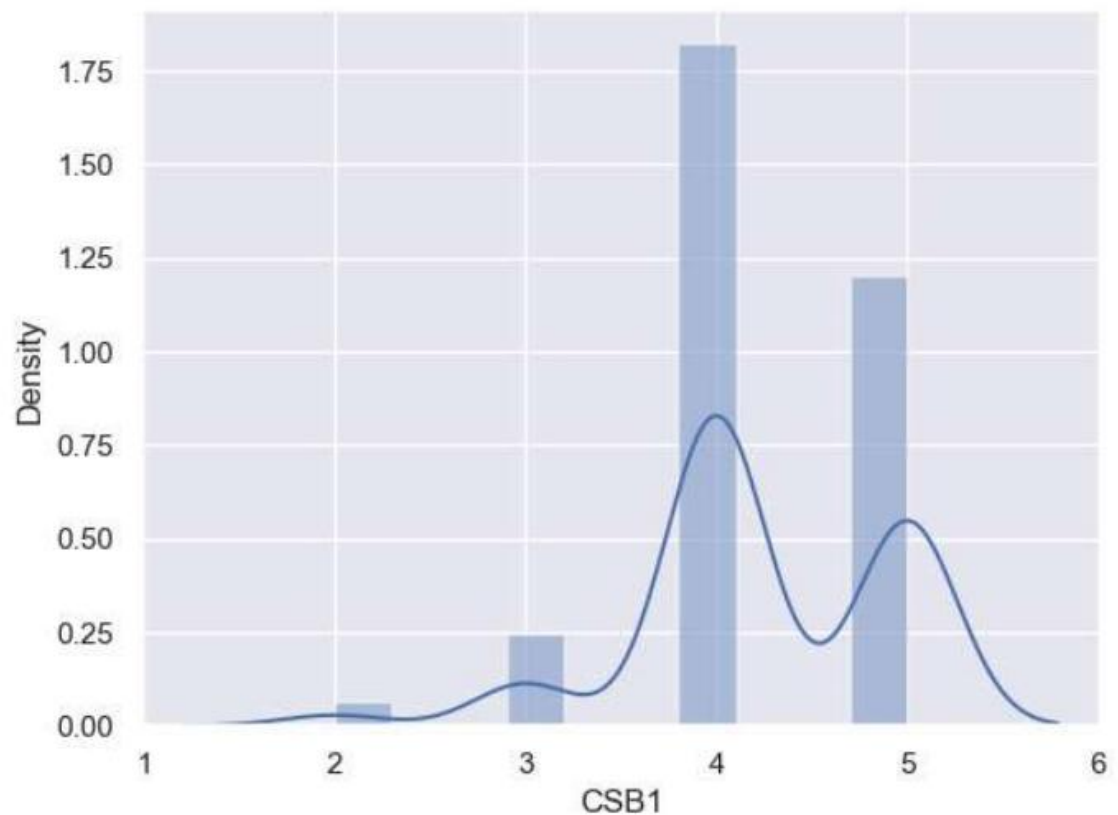


Figure 73: Cybersecurity Behavior

4.3.8. Research Hypothesis Testing

Considering the predictions provided by the machine learning pipeline, it is evident that all of the independent variables in this study that are mentioned and

explained in detail throughout the conceptual framework are positively influencing the culture of security in the banking sector.

Here is a table that summarizes the proposed hypotheses and their status:

Research Hypothesis	Status of Hypothesis
Hypothesis 1: External Influences Influence Cybersecurity Culture	Accepted
Hypothesis 2: Organizational Mechanisms Influence Cybersecurity Culture in Bahrain	Accepted
Hypothesis 3: Cybersecurity Culture influence Cybersecurity employee behavior in Bahrain	Accepted

Table 39: Research Hypothesis Testing

4.3.9. Preview of Research Study Results

A major objective of this research study is to evaluate cybersecurity culture's effects on Bahrain's banking sector, to analyze the external influences and internal mechanisms, to determine how cybersecurity culture affects employee behavior, and to provide suggestions to banks on how to improve cybersecurity culture for employee behavior.

To investigate the dependent variable (Cybersecurity Behavior), two independent variables are chosen (External Influences and Internal Mechanisms) and a moderator is selected (Cybersecurity Culture). Based on the results of the research conducted in this study, and according to the questions alluded to in Chapter 1 of this paper, the following questions can be clearly answered as a result of the interviews conducted by the researcher and his team:

Question 1: How is Bahrain's banking sector adopting cybersecurity culture through external influences and organizational mechanisms?

The information extracted from the structured closed-ended interview questions was input into Python to calculate the mean based on a Likert scale of 5 points. Based on the results of the questions relating to the external influences variable, the mean value is 4.435185185, which indicates participants agree or strongly agree to the questions regarding this factor of the cybersecurity culture context.

In contrast, SVC classifier's mean importance measure related to external influences is 0.0345986.

Question 2: How can machine learning methods contribute to Bahrain's banking sector adoption of cybersecurity culture?

As a result of coding the close-ended questions and entering them into a system using the Likert scale on a 5-point scale, the sample answers in the interviews, and after going through a detailed analysis of those responses. This research shows that the organizational mechanisms variables are 4.318181818 as the mean value. In other words, the participants in the study agree and strongly agree with the questions regarding the organizational mechanisms.

Question 3: What effect does cybersecurity culture have on banking employees' behavior?

Following the coding and entry of the closed-ended questions into a system that uses Likert scales on a 5-point scale, the sample answers from the interviews, and a detailed analysis of and review of those responses. In his study, the mean value for the cybersecurity culture moderator variable is 3.588624339. To summarize, the study participants strongly agreed and agreed with the questions relating to cybersecurity culture and employee behavior

4. 4. Chapter Summary

This study has several objectives, and the main objective of this research is to assess the effect of cybersecurity culture on employee behavior in banking sector in Bahrain. This chapter of the study included a detailed analysis of the findings from the structured close-ended interviews conducted, and it brings forward a detailed analysis of the interview questions, a detailed explanation of the variables of this research, the coding system of the interview questions to quantitatively measure the results of the findings.

Then this chapter covered a deep step-by-step analysis of the results using the machine learning pipeline and presented all the steps in extreme detail, with a vast representation of tables, graphs and acquired data from the SVC Classifier, which is the machine learning algorithm model used to acquire the outcomes herein.

The chapter ends by presenting the hypothesis and a preview of the questions deployed from the first chapter of this research.

All in all, the following table provides a summary of the machine pipeline used in this study:

Machine Learning Pipeline	What has been done	Results
Dataset Collection	Development of Interview Questions Structuring Interview Questions	Acquiring the Participation of 108 IT/Cybersecurity Workers in Bahrain in banking sector

	Inserting Questions into a Data Input System Conducting Interviews	
Data Preparation	Data is Reviewed Data is Entered into Excel and Cleaned Data is Imported into the Anaconda Python Program Data is Further Cleaned, Preprocessed, and Transformed to an Analysis Friendly Format.	Data is Ready to Input to the Learning Algorithm Model for Training and Testing Data is Accurate, Precise and Complete
Feature Engineering	Implementation of Correlation Removing Correlated Data Acquiring Mean & Standard Deviation of Results	3 Correlated Parameters are Removed
Selection of Model	Selection of the Supervised Learning, SVM Model Implementing the Entropy Splitting Feature Formula Acquiring the Average Accuracy Values of the 10 Different Machine Learning Models for Ensuring the	Selection of the SVM Model and Comparing Between Different Models. Accuracy Measure Shows that Random Forest has the Most Accurate Measure and is the Most Applicable for the Study.

	Selection of the Random Forest Model.	
Training the Model	The Stratified Sampling Technique is Used, the Data is Split into 2 Categories, the Training Data Subset (80% of the Data) and the Testing Data Subset (20% of the Data)	The Precision of the SVM is 94%
Model Evaluation	Usage of the Confusion Matrix Technique for Evaluating the SVM Model	Evaluation Concluded Where SVC Classifier Model Passed Evaluation and is Applicable to Being Used.
Prediction/ Deployment (Results)	The SVM Model Beings Working on the Entire Data Subset to Make Predictions and Extract the Importance Measurement Value of All Parameters Involved.	All Parameters Acquired a Value of Importance Measurement. The Mean Value of the Importance Measurement of Each Variable is Extracted. Acquisition of All Tables, Graphs, and Important Data Required for Research. The Acquisition of Decision Trees.

Table 35: Summary of the Study’s Machine Learning Pipeline

Chapter Five: Conclusion and Recommendations

5.1. Introduction

As the number of cybercrimes has increased over the past few years, cybersecurity has become one of the most serious global challenges that the entire world is facing. However, very few studies have examined the effects of cybersecurity culture on employee behavior. Technology has enabled the banking sector to leverage new opportunities, and the growth of technology has resulted in exposure, and policies for awareness are of utmost importance in banks, to maintain customers' trust and protect their data and money. In order to accomplish this, organizations must provide awareness and training programs to their employees. Having a secure information system requires a high level of awareness about cyber security.

Bahrain's banking sector lacks a clear understanding of how cybersecurity culture affects employee behavior. As part of this study, we examined the internal and external influences related to cybersecurity culture and how employee security behavior is influenced by cybersecurity culture. A recommendation for Bahrain's banking sector's stakeholders and decision-makers will also be developed.

This chapter summarizes the research paper's results and includes the concluding points in relation to the research. The following sections are included:

1. Introduction
2. The Theoretical and Practical Implications
3. Research Limitations
4. Suggestions for Future Researchers
5. Recommendations

6. Conclusion

5.2. The Theoretical and Practical Implications

This study investigates the relationship between external influences and internal mechanisms on cybersecurity culture, and the impact of cybersecurity culture on employee behavior within the banking sector in the Kingdom of Bahrain.

5.2.1. Theoretical Implications

As a result of the current study, there are many theoretical implications, which are summarized as follows:

1. Enhancing cybersecurity culture knowledge:

By exploring organizational cybersecurity culture in the context of banking sector in Bahrain, this study enhances knowledge about cybersecurity culture. It focuses particularly on enhancing employee security behavior.

2. Bridging the knowledge gap

As it provides precise and accurate predictions about cybersecurity culture impact on employees' security behaviors, this paper fills knowledge gaps concerning the field being discussed herein. Additionally, it gathers detailed historical data regarding the topic from literature and adjusts the theoretical framework to take into account the required factor, which is the budget.

3. Recognizing the Banking sector cybersecurity culture influencers

In this paper, the factors that influence cybersecurity culture in the banking sector are identified. It highlights how cybersecurity culture influences external and internal factors, and gives a concise explanation by examining the results of the study conducted in Bahrain; in addition, it emphasizes how cybersecurity culture can influence employee behavior.

4. Developing a better understanding of employee behavior in relation to cybersecurity culture

An understanding of the relationship between cybersecurity culture and employee behavior in Bahrain's banking sector is provided in this paper. As a result of this, it describes which settings are most conducive to high employee security behavior, and which settings have the least effect.

5. The future researcher's reference

Using this paper, future researchers will be able to acquire insight into other areas that science has not yet discovered in order to build and expand the research.

5.2.2. Practical Implications

As a result of the current study, there are many theoretical implications, which are summarized as follows:

1. Banking Sector Insights

As a result of this paper, Bahrain's banking sector will gain valuable insights into cybersecurity culture and how to build it in the organization. It also identifies the most influential factors so that organizations can concentrate on developing these influential factors. Additionally, this paper may provide organizations with knowledge that can be used to create policies, procedures, and codes of conduct that are in line with maintaining a high cybersecurity culture and high employee security behaviors.

2. Policy makers' guidance

As a source of informative knowledge, this paper provides policymakers in Bahrain with an opportunity to make informed decisions about their governments and politics. For Bahraini decision makers, this paper can provide evidence-based

insight that will assist them in building a high cybersecurity culture, especially when it comes to infrastructure development, work regulations, and other initiatives.

3. Create an inspiring environment for future researchers

In addition to discussing real-world possibilities, this paper demonstrates how it may be applied to various fields, especially in regard to researchers who may be interested in expanding this paper's data to further means in their respective fields of study.

Researchers will be able to use the results of this research to determine how the internal and external efficiency factors effect cyber security. The correlation between all the factors will be studied in future research in order to predict performance in cyber security.

4. Developing a broader perspective

The readers of this paper may be able to gain a better understanding of cyber security culture in Bahrain's banking sector and how it affects employee behavior, thus changing prior perceptions and adding new perspectives on the topic in Bahrain, and possibly the Gulf region at large.

Using our model, future researchers can:

- Take data from an organization that is specific to the model and validate it
- Create a model based on sectors
- Develop further models that correlate internal and external efficiency.

- Aid cyber security practitioners in focusing on relevant areas based on their particular business objectives and requirements

5.3. Research Limitations

There are some limitations to this research that might have affected its outcome:

1. Coronavirus – Pandemic

As a result of the COVID-19 pandemic, which lasted from 2019 until 2023, the researcher faced the first limitation. Since it was hard to move physically from one place to another during this period, some activities were abandoned and replaced with virtual approaches in order to achieve them, as follows are a few examples relating to how the pandemic affected the research activities:

- Having a physical meeting with the advisor
- Research visits to the University library
- The actual distribution of the survey and the distribution of samples during sampling were physically hampered.

The previous methods were replaced by electronic, and virtual means for obtaining results during the research.

2. The sample Size

In comparison to the size and importance of the research topic, the sample size for this study is relatively small, and this impacts the generalizability of findings; in fact, a larger, more diverse sample might provide a more comprehensive data outlook.

3. Specification of the context

Since this study is specifically related to Bahrain, it may be difficult to generalize it. As a result, the findings of this study may not be applicable to other nearby countries due to Bahrain's nature, which accommodates a diverse population that comes from a variety of backgrounds, ethnicities, religions, and such, which may not apply to other neighboring countries in the vicinity.

4. The lack of research in Bahrain

In terms of the main topic of this study, A Study of Cybersecurity Behavior among Bahraini Bank Employees, the researcher found a relatively limited number of studies related to the topic, which led the researcher to search for research papers related to studies conducted in other countries that differ entirely from the ones conducted in this country.

5.4. Suggestions for Future Researchers

This paper offers the following suggestions for future researchers interested in expanding on the methodology and findings of this study:

1. Studying longitudinally

In the future, it is suggested that researchers devote more time to conducting their research, especially in the areas and to acquiring more data in order to ensure a larger sample size and to obtain comprehensive results. In addition, it is important to understand how cybersecurity culture impacts employees' behavior over the long run.

2. Studies of Comparative Effectiveness

Researchers are encouraged to study how the cybersecurity culture impacts employee behavior, as this will provide more valuable data about the factors that contribute to cybersecurity culture and its effects on employee behavior. A high-

end researcher may also need to investigate this comparison between different industries. It may be the case that a high cybersecurity culture is more beneficial than a low cybersecurity culture, which may differ in other industries.

3. Aspects of Ethics

A research study on employee security behavior should also consider investigating the role of ethics. Researchers may find that employees who demonstrate high ethical consideration are likely to perform better in relation to cybersecurity compared with those who demonstrate low ethical consideration. Alternatively, high ethical consideration employees might actually perform worse than their counterparts due to a lack of security compliance

5.5. Recommendations

This research, which came to a variety of conclusions, provides plenty of recommendations for readers to acquire. The recommendations provided below are based on the conclusions reached by the study.

1. Investing in infrastructure

For organizations seeking to enhance their cybersecurity culture, it is recommended they invest in improving their technological infrastructure by providing employees with the tools needed for effective communication, efficient task management, and efficient collaboration. An employee's productivity won't be hindered by a platform that they find reliable.

Improvements must be made to the existing IT infrastructure to enable new technologies and security updates for legacy hardware and software components to be implemented readily

2. Creating clear guidelines

In order for employees to know what is expected of them when working in an office setting, it is recommended that organizations develop a booklet that has clear guidelines on cybersecurity culture. Setting goals is recommended as SMART (Specific, Measurable, Achievable, Realistic, and Timely), emphasizing the realistic part. Several previous studies and this study have found that supervisors typically assign employees unrealistic goals. Considering that technology is constantly changing and improving, organizations should also continue to solicit feedback from their employees in order to develop these guidelines further. It is also important to provide employees with an employee handbook with clear guidelines and guidelines that they can refer to in order to comply with the requirements on time.

3. Implementing Effective Cybersecurity

In order to ensure an effective cybersecurity implementation in an organization, organizations should examine the factors influencing the implementation of cybersecurity, including cybersecurity strategies, insurance, intelligence, worksheets, protocols, and standards. All of these factors can influence an organization's cybersecurity culture.

4. Keeping up to date

Organizations should continue to work on updating their technological tools and this can be accomplished by being aware of current trends, emerging technologies, and the best practices related to cybersecurity culture. An organization that neglects this approach may find in a short period that its employees are switching jobs since other firms are more technologically advanced and better able to accommodate them.

5.6. Conclusion

As a conclusion to this research, this study examines how cyber security culture impacts employee behavior. It examines both external factors and internal mechanisms that influence cyber security culture.

During the course of conducting this research, we did not find any studies related to the same topic as this study in the context of Bahrain, however, studies from around the world provided valuable insights about the impact of cybersecurity culture on employee behavior. Due to the increased number of cybercrimes over the last few years, cybersecurity is perceived as one of the most serious global issues the entire world faces, however, very few research projects have been conducted on cybersecurity culture, while the banking sector has leveraged new technologies. In the banking sector, policies for awareness have become increasingly important, as technology has grown. In order to maintain customer trust, it is important to protect customers' money and data. This can be accomplished by implementing awareness and training programs within the organization. It is imperative for any organization to prioritize cyber security awareness so that its information systems are secure. A major problem with this study lies in a lack of understanding of cybersecurity employee behavior in the Bahraini Banking Sector; the purpose of this study is to determine what factors influence the cybersecurity culture of banks, and to develop recommendations for relevant stakeholders and decision makers in the Bahraini banking industry.

In terms of the theoretical framework, this study presents a variety of research variables, including independent, moderator and dependent variables. There are

two independent variables associated with cybersecurity culture: external influence factors and internal mechanisms factors. Cybersecurity culture is the moderator variable, and employee cybersecurity behavior is the dependent variable. As for the research design philosophy, positivism and interpretivism are the research philosophies adopted in this study, and a quantitative research design philosophy is used. This methodology includes data acquisition based on structured close-ended questions conducted with random participants from the population through the use of structured closed-ended interviews. This interview questions were derived from a previous literature survey and developed further by the researcher to include the context of new technologies that were emerging at the time that the referenced paper was written, as well as Bahrain's context. The interviewers inputted the data from the interviewees in an automated method using Google Forms Online Platform, each question was coded for easy quantification, and the questions used a 5-point Likert Scale to assess each.

This study conducted 108 interviews and achieved a 100% response rate because interviewers were trained to carefully ask questions and inform participants that the interviews are anonymous. As part of this study, machine learning pipelines are deployed in its analysis, which consist of several steps that assist computers in making predictions and decisions, with high accuracy, precision, and no errors. Using supervised learning techniques and SVM algorithms, the machine learning approach uses supervised learning techniques. Using the entropy feature of the SVM, this approach splits the data within the SVM, and Python is used for programming. According to the results of the interview, 57.4% of the sample are female, 42.6% are male, and 54.6% are between the ages of 30 and 39. In addition, 50% of the sample has a marriage with children, while 37% are single, and 88.9% of the sample holds a bachelor's degree. In order to implement the machine learning pipeline, data collection, data preparation, feature engineering, model selection, model training, model evaluation, hyper parameters, and prediction were

all conducted through a well-structured process. In the first step, data collection was conducted through interviews, and the data gathered from the interviews were analyzed. Following the cleaning and review, the acquired data was input into the system and reviewed to ensure no errors had occurred. After selecting the machine learning feature, the supervised SVM algorithm with the entropy feature was selected. Based on the datasets and a stratified sampling technique, the model has been trained and tested; its settings have been further adjusted during the evaluation phase resulting in a good model for application. This model extracted the importance measure for each parameter and presented the data in a visual way, with tables and graphs, and included detailed discussion. According to the values obtained in this study (external influences and internal mechanisms), cybersecurity culture is influenced by all the independent variables. In the context of cybersecurity culture, it is surprising that the external influences factors have the lowest influence, while the organizational mechanisms play the highest role in influencing cybersecurity culture. As for the moderator variable, cybersecurity culture, it appears that it influences employee cybersecurity behavior and intention to act.

In conclusion, this study has many theoretical and practical implications, including the advancement of knowledge about cybersecurity culture in the banking work context, as well as identifying the influencers influencing cybersecurity culture in the banking work context and providing a clear understanding of the relationship between employee behavior and cybersecurity culture. The practical implications of this study, on the other hand, include providing insights to organizations, using this study as guidance for policy makers, providing inspiration for future research, and broadening perspectives. Despite this, the research had some limitations that prevented it from being as generalizable as possible, such as the COVID-19

pandemic, the small sample size, and the lack of previous research in Bahrain. Finally, a number of recommendations are made to organizations, practitioners, readers, and other stakeholders in this paper, including investment in technological infrastructure, developing clear guidelines, ensuring employees receive continuous cybersecurity training and staying updated with the latest cybersecurity trends, technologies, tools, and best practices, and implementing effective cybersecurity.

References

1. Abdalla, M., Jarrah, M., Abu-Khadrah, A., & Arshad, Y. bin. (2021a). Factors influencing the adoption of cyber security standards among public listed companies in Malaysia. *International Journal of Advanced Computer Science and Applications*, 12(11). <https://doi.org/10.14569/ijacsa.2021.0121191>
2. Abdulkareem, Mohammed. (2012). “Bahraini Firms Facing Cyber Attack Threats.” Bahrain Institute of Banking and Finance senior IT support engineer Mohammed Abdulkareem was interviewed in Dilmun-Times on 22 July 2012. Retrieved January 24, 2018. From: <http://www.dilmun-Times.com/?p=22072>
3. Abu Afifa, M. M., Vo Van, H., & Le Hoang Van, T. (2022). Blockchain adoption in accounting by an extended UTAUT model: Empirical evidence from an emerging economy. *Journal of Financial Reporting and Accounting*, 21(1), 5–44. <https://doi.org/10.1108/jfra-12-2021-0434>
4. Abu-Mostafa, Y. S., Magdon-Ismail, M. & Lin, H. T., 2012. *Learning from data*. s.l.:Springer Science & Business Media.
5. Abutabenjeh, S., & Jaradat, R. (2018). Clarification of research design, Research Methods, and research methodology. *Teaching Public Administration*, 36(3), 237–258. <https://doi.org/10.1177/0144739418775787>
6. Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction*, 29(3), 701–750. <https://doi.org/10.1007/s11257-019-09236-5>
7. Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction*, 29(3), 701–750. <https://doi.org/10.1007/s11257-019-09236-5>

8. Agboola, M. G., Akinbode, M., Segun-Adeniran, C., Ifeanyichukwu Dibia, P., Oloruntoba, A., Dinyain, T., Johnson Fabunmi, T., Funsho, T., Abayomi Akinde, O., & Betek, C. M. (2019). Technology usage and employee behaviour: Controversies, complications, and implications in the Nigerian Business Environment. *IOP Conference Series: Earth and Environmental Science*, 331(1), 012031. <https://doi.org/10.1088/1755-1315/331/1/012031>
9. Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies*, 2(4), 314–324. <https://doi.org/10.1002/hbe2.195>
10. Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, 136, 107376. <https://doi.org/10.1016/j.chb.2022.107376>
11. Alawi, A. I. (2006). Investigating the strategies for successful development of Health Information Systems: A comparison study. *Information Technology Journal*, 5(4), 626–647. <https://doi.org/10.3923/itj.2006.626.647>
12. Alazab, M., Alhyari, S., Awajan, A., & Abdallah, A. B. (2020). Blockchain technology in Supply Chain Management: An empirical study of the factors affecting user adoption/acceptance. *Cluster Computing*, 24(1), 83–101. <https://doi.org/10.1007/s10586-020-03200-4>
13. Al-Hamar, A. K. (2016, March). Enhancing Information Security Process in Organisations in Qatar. In *Qatar Foundation Annual Research Conference Proceedings* (Vol. 2016, No. 1, p. ICTPP2531). Qatar: HBKU Press.
14. Ali, Z. L., Hayale, W. S., Al_Barazanchi, I. I., Sekhar, R., Shah, P., & Parihar, S. (2024a). Efficient cybersecurity assessment using SVM and fuzzy evidential reasoning for resilient infrastructure. *Ingénierie Des Systèmes d'Information*, 29(2), 515–521. <https://doi.org/10.18280/isi.290212>

15. Almaiah, M. A., Almomani, O., Al-Khasawneh, A., & Althunibat, A. (2021). Predicting the acceptance of mobile learning applications during COVID-19 using machine learning prediction algorithms. *Studies in Systems, Decision and Control*, 319–332. https://doi.org/10.1007/978-3-030-67716-9_20
16. Al-Marroof, R. A., Arpaci, I., Al-Emran, M., Salloum, S. A., & Shaalan, K. (2020). Examining the acceptance of WhatsApp stickers through Machine Learning Algorithms. *Studies in Systems, Decision and Control*, 209–221. https://doi.org/10.1007/978-3-030-47411-9_12
17. Al-Maskati, H. (2016, May 24). CBB Cyber Security Workshop. Al-Maskati, Executive Director - Corporate Services, Central Bank of Bahrain, Keynote Address, Retrieved January 21, 2018, from http://www.cbb.gov.bh/page-pcbb_cyber_security_workshop.htm
18. Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(3), 176-183.
19. Alqahtani, H., & Kavakli-Thorne, M. (2020b). Exploring factors affecting user's cybersecurity behaviour by using Mobile Augmented Reality App (CybAR). *Proceedings of the 2020 12th International Conference on Computer and Automation Engineering*. <https://doi.org/10.1145/3384613.3384629>
20. Alqahtani, H., Kavakli-Thorne, M., & Alrowaily, M. (2020). The impact of gamification factor in the acceptance of Cybersecurity Awareness Augmented Reality Game (cybar). *HCI for Cybersecurity, Privacy and Trust*, 16–31. https://doi.org/10.1007/978-3-030-50309-3_2
21. Alqahtani, M., & Braun, R. (2021a). Reviewing influence of UTAUT2 factors on Cyber Security Compliance: A literature review. *Journal of Information*

- Assurance & Cybersecurity, 2021, 1–15.
<https://doi.org/10.5171/2021.666987>
22. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98, 102003.
<https://doi.org/10.1016/j.cose.2020.102003>
 23. Alwabel, A. S., & Zeng, X.-J. (2021). Data-driven modeling of Technology Acceptance: A machine learning perspective. *Expert Systems with Applications*, 185, 115584. <https://doi.org/10.1016/j.eswa.2021.115584>
 24. Alzighaibi, A. R. (2021). Cybersecurity attacks on academic data and personal information and the mediating role of Education and employment. *Journal of Computer and Communications*, 09(11), 77–90.
<https://doi.org/10.4236/jcc.2021.911006>
 25. Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., & Choudrie, J. (2021). Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile Workforce. *Computers in Human Behavior*, 114, 106531. <https://doi.org/10.1016/j.chb.2020.106531>
 26. Andeme Bikoro, D. M., Fosso Wamba, S., & Kala Kamdjoug, J. R. (2018). Determinants of cyber security use and behavioral intention: Case of the Cameroonian Public Administration. *Advances in Intelligent Systems and Computing*, 1087–1096. https://doi.org/10.1007/978-3-319-77712-2_104
 27. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443. <https://doi.org/10.1016/j.chb.2016.12.040>
 28. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443. doi:10.1016/j.chb.2016.12.040

- 29.Argote, L. (2011). Organizational Learning Research: Past, present and future. *Management Learning*, 42(4), 439–446. <https://doi.org/10.1177/1350507611408217>
- 30.Atoum, I., Ootom, A., & Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, 22(3), 251–264. <https://doi.org/10.1108/imcs-02-2013-0014>
- 31.Avci, I., & Koca, M. (2023). Cybersecurity attack detection model, using Machine Learning Techniques. *Acta Polytechnica Hungarica*, 20(7), 29–44.<https://doi.org/10.12700/aph.20.7.2023.7.2>
- 32.Babbie, E. R., 2017. Basics of Social Research. s.l.:Cengage Learning.
- 33.Basias, N. & Pollalis, Y., 2018. Quantitative and qualitative research in business & technology: Justifying a suitable research methodology. *Review of Integrative Business and Economics Research*, Volume 7, pp. 91-105.
- 34.Basten, D., & Haamann, T. (2018). Approaches for organizational learning: A literature review. *SAGE Open*, 8(3), 215824401879422. <https://doi.org/10.1177/2158244018794224>
- 35.Bergstra, J. & Bengio, Y., 2012. Random search for hyper-parameter optimization. *Journal of Machine Learning Research*, Volume 13, pp. 281-305.
- 36.Bergstra, J., Komer, B., Eliasmith, C., Yamins, D., & Cox, D. D. (2015). Hyperopt: A python library for model selection and hyperparameter optimization. *Computational Science & Discovery*, 8(1), 014008. <https://doi.org/10.1088/1749-4699/8/1/014008>
- 37.Beuran, R., Chinen, K. I., Tan, Y., & Shinoda, Y. (2016). Towards effective cybersecurity education and training.
- 38.Beuran, R., Pham, C., Tang, D., Chinen, K.-ichi, Tan, Y., & Shinoda, Y. (2017).

Cytrone: An integrated cybersecurity training framework. Proceedings of the 3rd International Conference on Information Systems Security and Privacy. <https://doi.org/10.5220/0006206401570166>

39. Bizbahrain (2015), TRA Heads Bahrain's Delegation to US-GCC Cyber Security Strategic Cooperation Forum, September 15, 2015, [online], [Retrieved August 3, 2016] <http://www.bizbahrain.com/tra-heads-bahrain-delegation-to-us-gcc-cybersecurity-strategic-cooperation-forum/>.
40. Boonsiritomachai, W., & Pitchayadejanant, K. (2017). Determinants affecting mobile banking adoption by generation Y based on the unified theory of acceptance and use of technology model modified by the Technology Acceptance Model Concept. *Kasetsart Journal of Social Sciences*. <https://doi.org/10.1016/j.kjss.2017.10.005>
41. Branley-Bell, D., Coventry, L., & Sillence, E. (2021a). Promoting cybersecurity culture change in healthcare. The 14th Pervasive Technologies Related to Assistive Environments Conference. <https://doi.org/10.1145/3453892.3461622>
42. Braun, V., Clarke, V. & Weate, P., 2017. Using thematic analysis in sport and exercise research. s.l.:Routledge
43. Breiman, L., 2001. Random forests. *Machine learning*, 45(1), pp. 5-32.
44. Bronk, C., & Tikk-Ringas, E. (2013). The cyber-attack on Saudi Aramco. *Survival*, 55(2), 81–96. <https://doi.org/10.1080/00396338.2013.784468>
45. Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU the example of the financial sector: A legal perspective. *German Law Journal*, 21(6), 1149–1179. <https://doi.org/10.1017/glj.2020.67>
46. Chandra, A., & Snowe, M. J. (2020). A taxonomy of cybercrime: Theory and design. *International Journal of Accounting Information Systems*, 38, 100467. <https://doi.org/10.1016/j.accinf.2020.100467>

- 47.Chang, A. (2012). Utaut and utaut 2: A review and agenda for future research. *The Winners*, 13(2), 10. <https://doi.org/10.21512/tw.v13i2.656>
- 48.Charmaz, K., 2014. Constructing grounded theory. s.l.:Sage.
- 49.Chatfield, A. T., & Reddick, C. G. (2017). Cybersecurity innovation in Government. *Proceedings of the 18th Annual International Conference on Digital Government Research*. <https://doi.org/10.1145/3085228.3085233>
- 50.Chauhan, S., Mittal, M., Woźniak, M., Gupta, S., & Pérez de Prado, R. (2021). A technology acceptance model-based analytics for online mobile games using Machine Learning Techniques. *Symmetry*, 13(8), 1545. <https://doi.org/10.3390/sym13081545>
- 51.Chauhan, V. K., Dahiya, K., & Sharma, A. (2018). Problem formulations and solvers in Linear SVM: A Review. *Artificial Intelligence Review*, 52(2), 803–855. <https://doi.org/10.1007/s10462-018-9614-6>
- 52.Chea, S., & Luo, M. M. (2019). Pleasantness, activation, and negative affectivity: A test of extended utaut model. *Proceedings of the Annual Hawaii International Conference on System Sciences*. <https://doi.org/10.24251/hicss.2019.616>
- 53.Cheng, L., Liu, F., & Yao, D. D. (2017). Enterprise data breach: Causes, challenges, prevention, and Future Directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7(5). <https://doi.org/10.1002/widm.1211>
- 54.Chia, R. (2002). The production of management knowledge: Philosophical underpinnings of research design. *Essential Skills for Management Research*, 2–19. <https://doi.org/10.4135/9781848605305.n1>

55. Chung, W., Chen, H., Chang, W., & Chou, S. (2006). Fighting cybercrime: A review and the Taiwan Experience. *Decision Support Systems*, 41(3), 669–682. <https://doi.org/10.1016/j.dss.2004.06.006>
56. Clark-Ginsberg, A., & Slayton, R. (2018). Regulating risks within complex sociotechnical systems: Evidence from Critical Infrastructure Cybersecurity Standards. *Science and Public Policy*, 46(3), 339–346. <https://doi.org/10.1093/scipol/scy061>
57. Creswell, J. W. & Creswell, J. D., 2017. Research design: Qualitative, quantitative, and mixed methods approaches. s.l.:Sage publications.
58. Creswell, J. W., 2014. Research Design: Qualitative, Quantitative, and Mixed Methods. SAGE Publications, Inc. ed. Thousand Oaks, CA: 4.
59. D. J., C. & Connelly, F. M., 2000. Narrative inquiry: Experience and story in qualitative research. s.l.:Jossey-Bass..
60. Da Veiga, A. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. 2016 SAI Computing Conference (SAI). <https://doi.org/10.1109/sai.2016.7556102>
61. Dasgupta, D., Akhtar, Z., & Sen, S. (2020). Machine learning in cybersecurity: A comprehensive survey. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 19(1), 57–106. <https://doi.org/10.1177/1548512920951275>
62. David, 2019. What is the difference between population and sample?. [Online] Available at: <https://www.statisticssolutions.com/what-is-the-difference-betweenpopulation-and-sample/> [Accessed 30 4 2023].
63. Dedeke, A., & Masterson, K. (2019). Contrasting cybersecurity implementation frameworks (CIF) from Three countries. *Information & Computer Security*, 27(3), 373–392. <https://doi.org/10.1108/ics-10-2018-0122>

64. Dietterich, T. G., 1998. Approximate statistical tests for comparing supervised classification learning algorithms. *Neural computation*, 10(7), pp. 1895-1923.
65. Donalds, C., & Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51, 102056. <https://doi.org/10.1016/j.ijinfomgt.2019.102056>
66. Draelos, R., 2019. *Measuring Performance: The Confusion Matrix*. [Online] Available at: <https://glassboxmedicine.com/2019/02/17/measuring-performance-theconfusion-matrix/> [Accessed 13 5 2023].
67. Emekci, S. (2019). Green consumption behaviours of consumers within the scope of TPB. *Journal of Consumer Marketing*, 36(3), 410–417. <https://doi.org/10.1108/jcm-05-2018-2694>
68. Gao, L., Calderon, T. G., & Tang, F. (2020). Public companies' cybersecurity risk disclosures. *International Journal of Accounting Information Systems*, 38, 100468. <https://doi.org/10.1016/j.accinf.2020.100468>
69. Gcaza, N., & von Solms, R. (2017). A strategy for a cybersecurity culture: A south african perspective. *The Electronic Journal of Information Systems in Developing Countries*, 80(1), 1–17. <https://doi.org/10.1002/j.1681-4835.2017.tb00590.x>
70. Genuer, R., Poggi, J. M. & Tuleau-Malot, C., 2010. Variable selection using random forests. *Pattern Recognition Letters*, 31(14), pp. 2225-2236.
71. Ghanem, K., Aparicio-Navarro, F. J., Kyriakopoulos, K. G., Lambotharan, S., & Chambers, J. A. (2017). Support Vector Machine for network intrusion and Cyber-Attack detection. *2017 Sensor Signal Processing for Defence Conference (SSPD)*. <https://doi.org/10.1109/sspd.2017.8233268>
72. Ghiasi, et al., 2022. A Comprehensive Review of Random Forest Algorithm: Research Progresses, Limitations, and Future Directions. *IEEE Access*.

73. Goodfellow, I., Bengio, Y. & Courville, A., 2016. Deep learning. s.l.:MIT Jovel, J. & Greiner, R., 2021. An introduction to machine learning approaches for biomedical research. *Frontiers in Medicine*, Volume 8, p. 2534. [Press.
74. Gordon, S., & Ford, R. (2006). On the definition and classification of Cybercrime. *Journal in Computer Virology*, 2(1), 13–20. <https://doi.org/10.1007/s11416-006-0015-z>
75. Gumusbas, D., Yldrm, T., Genovese, A., & Scotti, F. (2021). A comprehensive survey of databases and deep learning methods for cybersecurity and Intrusion Detection Systems. *IEEE Systems Journal*, 15(2), 1717–1731. <https://doi.org/10.1109/jsyst.2020.2992966>
76. Gunjan, V. K., Kumar, A., & Avdhanam, S. (2013). A survey of Cyber Crime in India. 2013 15th International Conference on Advanced Computing Technologies (ICACT). <https://doi.org/10.1109/icact.2013.6710503>
77. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in Accounting Research. *SSRN Electronic Journal*. doi:10.2139/ssrn.3923245
78. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in Accounting Research. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3923245>
79. Hassan, L. M., Shiu, E., & Parry, S. (2015). Addressing the cross-country applicability of the theory of planned behaviour (TPB): A Structured Review of multi-country TPB Studies. *Journal of Consumer Behaviour*, 15(1), 72–86. <https://doi.org/10.1002/cb.1536>
80. Ho, H., Ko, R., & Mazerolle, L. (2022). Situational Crime Prevention (SCP) techniques to prevent and Control Cybercrimes: A focused systematic review. *Computers & Security*, 115, 102611. doi:10.1016/j.cose.2022.102611
81. Houston, K., 2022. Quantitative data-collection methods. [Online] Available at: <https://www.jotform.com/blog/quantitative-data->

collectionmethods/#:~:text=Interviews,for%20responses%20with%20detailed%20context. [Accessed 13 5 20236].

- 82.Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. Proceedings of the Annual Hawaii International Conference on System Sciences. <https://doi.org/10.24251/hicss.2019.769>
- 83.Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. Proceedings of the Annual Hawaii International Conference on System Sciences. <https://doi.org/10.24251/hicss.2019.769>
- 84.Islam, R., & Rasad, S. bin. (2005). Employee performance evaluation by AHP: A case study. *Proceedings of the International Symposium on the Analytic Hierarchy Process*. <https://doi.org/10.13033/isahp.y2005.028>
- 85.Johnson, A. L. (2016 b). Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation. NC Banking Inst., 20, 277.
- 86.Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, Perspectives, and prospects. *Science*, 349(6245), 255–260. <https://doi.org/10.1126/science.aaa8415>
- 87.Jovel, J. & Greiner, R., 2021. An introduction to machine learning approaches for biomedical research. *Frontiers in Medicine*, Volume 8, p. 2534.
- 88.Kabir, M. R., & Islam, M. A. (2021a). Behavioural intention to adopt blockchain technology in Bangladeshi banking companies. PROCEEDINGS OF 8TH INTERNATIONAL CONFERENCE ON ADVANCED MATERIALS ENGINEERING & TECHNOLOGY (ICAMET 2020). <https://doi.org/10.1063/5.0051654>

- 89.Kajal, A., & Nandal, S. K. (2020). A hybrid approach for cyber security: Improved intrusion detection system using ANN-SVM. *Indian Journal of Computer Science and Engineering*, 11(4), 412–425. <https://doi.org/10.21817/indjcse/2020/v11i4/201104300>
- 90.Kaplan, R. M. & Saccuzzo, D. P., 2017. Descriptive and inferential statistics; Psychological Testing: Principles, Applications, and Issues. 9 ed. s.l.:Cengage Learning.
- 91.KDnuggets, 2021. Poll Results: Which Data Science/Machine Learning tools you used in the past 12 months?. [Online] Available at: <https://www.kdnuggets.com/2019/05/new-poll-software-analytics-datascience-machine-learning.html> [Accessed 7 5 2023].
- 92.Kianpour, M., Kowalski, S. J., & Øverby, H. (2022). Advancing the concept of cybersecurity as a public good. *Simulation Modelling Practice and Theory*, 116, 102493. <https://doi.org/10.1016/j.simpat.2022.102493>
- 93.Kitto, S. C., Chesters, J., & Grbich, C. (2008). Quality in qualitative research. *Medical Journal of Australia*, 188(4), 243–246. <https://doi.org/10.5694/j.1326-5377.2008.tb01595.x>
- 94.Komer, B., Bergstra, J., & Eliasmith, C. (2014). Hyperopt-Sklearn: Automatic hyperparameter configuration for Scikit-Learn. *Proceedings of the Python in Science Conference*. <https://doi.org/10.25080/majora-14bd3278-006>
- 95.Krishna, B., Krishnan, S., & Sebastian, M. P. (2022). Examining the relationship between National Cybersecurity Commitment, culture, and digital payment usage: An Institutional Trust Theory Perspective. *Information Systems Frontiers*. <https://doi.org/10.1007/s10796-022-10280-7>
- 96.Krutz, R. L., & Vines, R. D. (2001). The CISSP prep Guide: Mastering the ten domains of Computer Security (pp. 183-213). New York: Wiley.

97. Kshetri, N. (2016). The Quest to Cyber Superiority. <https://doi.org/10.1007/978-3-319-40554-4>
98. Kulkarni, A., Chong, D. & Batarseh, F. A., 2020. Foundations of data imbalance and solutions for a data democracy.. *Data Democracy*, pp. 83-106.
99. Kumar, A. & Kim, J. H., 2017. Machine learning approaches for cancer classification and prediction. *Applied Sciences*, 7(10), p. 1064.
100. Kumar, R., 2015. Research Methodology: A Step-by-Step Guide for Beginners.. s.l.:Sage Publications.
101. Lee, I. (2021). Cybersecurity: Risk Management Framework and Investment Cost Analysis. *Business Horizons*, 64(5), 659–671. <https://doi.org/10.1016/j.bushor.2021.02.022>
102. Lehto, M. (2013). The cyberspace threats and cyber security objectives in the Cyber Security Strategies. *International Journal of Cyber Warfare and Terrorism*, 3(3), 1–18. <https://doi.org/10.4018/ijcwt.2013070101>
103. Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13-24. doi:10.1016/j.ijinfomgt.2018.10.017
104. Li, Y., Huang, J., Yang, J. & Jin, R., 2018. Feature engineering for machine learning: a comprehensive overview. s.l.:Springer.
105. Liaw, A. & Wiener, M., 2002. Classification and regression by randomForest. *R news*, 2(3), pp. 18-22.
106. Loi, M., Christen, M., Kleine, N., & Weber, K. (2019). Cybersecurity in health – disentangling value tensions. *Journal of Information, Communication and Ethics in Society*, 17(2), 229–245. <https://doi.org/10.1108/jices-12-2018-0095>

107. Mantha, B. R., Menassa, C. C. & Kamat, V. R., 2016. A taxonomy of data types and data collection methods for building energy monitoring and performance simulation.. *Advances in Building Energy Research*, 10(2), pp. 263-293.
108. Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Review: Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, 10(10), 2823–2836. <https://doi.org/10.1007/s13042-018-00906-1>
109. Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Review: Machine learning techniques applied to cybersecurity. *International Journal of Machine Learning and Cybernetics*, 10(10), 2823–2836. <https://doi.org/10.1007/s13042-018-00906-1>
110. Miller, J., Goyal, N. & Wice, M., 2015. Ethical considerations in research on human development and culture. *The Oxford handbook of human development and culture*, pp. 14-27.
111. Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes impacting cybersecurity policy development: An evidence from Seven nations. *Computers & Security*, 120, 102820. <https://doi.org/10.1016/j.cose.2022.102820>
112. Mitchell, T. M., 1997. *Machine learning*. s.l.:McGraw Hill.
113. Mohanty, R. P., & Dube, D. P. (2020). The application of Cyber Security Capability Maturity Model to identify the impact of internal efficiency factors on the external effectiveness of cyber security. *International Journal of Business Information Systems*, 1(1), 1. <https://doi.org/10.1504/ijbis.2020.10042363>
114. Mohd Ariffin, N. H., Ahmad, F., & Mohd Haneef, U. (2020). Acceptance of mobile payments by retailers using UTAUT model. *Indonesian Journal of*

- Electrical Engineering and Computer Science, 19(1), 149.
<https://doi.org/10.11591/ijeecs.v19.i1.pp149-155>
115. Mustafa Abdullah, D., & Mohsin Abdulazeez, A. (2021). Machine learning applications based on SVM classification a Review. *Qubahan Academic Journal*, 1(2), 81–90. <https://doi.org/10.48161/qaj.v1n2a50>
 116. Nabella, S. D., Rivaldo, Y., Kurniawan, R., Nurmayunita, Sari, D. P., Luran, M. F., Amirullah, Saputra, E. K., Rizki, M., Sova, M., Nurhayati, & Wulandari, K. (2022). The influence of leadership and organizational culture mediated by organizational climate on governance at senior high school in Batam City. *Journal of Educational and Social Research*, 12(5), 119. <https://doi.org/10.36941/jesr-2022-0127>
 117. Ng, K. C., Zhang, X., Thong, J. Y., & Tam, K. Y. (2021a). Protecting against threats to information security: An attitudinal ambivalence perspective. *Journal of Management Information Systems*, 38(3), 732–764. <https://doi.org/10.1080/07421222.2021.1962601>
 118. Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA – Journal of Business and Public Administration*, 9(3), 71–88. <https://doi.org/10.2478/hjbpa-2018-0024> November 28, 2017, from <http://www.newsofbahrain.com/viewNews.php?ppId=31499&TYPE=Posts&pid=21 &MNU=2&SUB>
 119. Okaily, M. A., Rahman, M. S., Ali, A., Shanab, E. A., Ra', N. A., Masa', ed, & deh, N. A. (2023). An empirical investigation on acceptance of Mobile Payment System Services in Jordan: Extending UTAUT2 model with security and privacy. *International Journal of Business Information Systems*, 42(1), 123. <https://doi.org/10.1504/ijbis.2023.128306>

120. Omar, M. M., Messaadia, M. & Elmezughi, A. M., 2023. Decision Tree and Random Forest Models for Internal Audit Effectiveness Factors Evaluation. 2023 International Conference on Cyber Management and Engineering (CyMaEn), pp. 214-217.
121. Palinkas, L. A. et al., 2015. Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5), pp. 533-544.
122. Ragin, C. C., 2017. *The comparative method: Moving beyond qualitative and quantitative strategies*. s.l.:Univ of California Press.
123. Raiu, C, Habini, M.A, Belov, S. and Mineev, M (2017), From Shamoon to StoneDrill - Wipers attacking Saudi organizations and beyond, Kaspersky Lab Report. Retrieved 21 January 2018 from: <https://securelist.com/from-shamoon-to-stonedrill/77725>
124. Rashed Mohamed Al Humaid Alneyadi, M., & Kassim Normalini, M. (2023). Factors influencing user's intention to adopt AI-based cybersecurity systems in the UAE. *Interdisciplinary Journal of Information, Knowledge, and Management*, 18, 459–486. <https://doi.org/10.28945/5166>
125. Reegård, K., Blackett, C., & Katta, V. (2019). The concept of cybersecurity culture. *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*. https://doi.org/10.3850/978-981-11-2724-3_0761-cd
126. Reeves, S., Kuper, A., & Hodges, B. D. (2008). Qualitative research methodologies: Ethnography. *BMJ*, 337(aug07 3). <https://doi.org/10.1136/bmj.a1020>
127. Rhodes, J. D. et al., 2014. Experimental and data collection methods for a large-scale smart grid deployment: Methods and first results. *Energy*, Volume

65, pp. 462-471.

128. Robles-Gómez, A., Tobarra, L., Pastor-Vargas, R., Hernández, R., & Cano, J. (2020). Emulating and evaluating Virtual Remote Laboratories for Cybersecurity. *Sensors*, 20(11), 3011. <https://doi.org/10.3390/s20113011>
129. Roulston, K. & Williams, M., 2017. Sampling in qualitative research: Ethical and practical considerations. *Journal of the Association for Information Science and Technology*, 68(9), pp. 2248-2254.
130. Saunders, M., Lewis, P. & Thornhill, A., 2019. Research methods for business students. 8 ed. Harlow, England: Pearson Education Limited
131. Saunders, V., McArthur, M. & Moore, T., 2015. Not seen and not heard: Ethical considerations of research with children of prisoners. *Law Context: A Socio-Legal J.*, Volume 32, p. 108.
132. Sebola, M. P., & Mamabolo, M. A. (2020). Governing and managing communal land as a resource in South Africa: A case of selected communal property associations in Vhembe District, Limpopo Province. *The Business and Management Review*, 11(01). <https://doi.org/10.24052/bmr/v11nu01/art-01>
133. Sekaran, U. & Bougie, R., 2016. Research methods for business: a skill-building approach. s.l.:John Wiley & Sons.
134. Shevade, S. K., Keerthi, S. S., Bhattacharyya, C., & Murthy, K. R. K. (2000). Improvements to the SMO algorithm for SVM regression. *IEEE Transactions on Neural Networks*, 11(5), 1188–1193. <https://doi.org/10.1109/72.870050>
135. Shihan, K. H., & Radif, M. J. (2022). Internal and external factors to adopt a cyber security strategy in Iraqi organisations. *Webology*, 19(1), 5181–5198. <https://doi.org/10.14704/web/v19i1/web19349>

136. Smith, K. T., Jones, A., Johnson, L., & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society*, 17(1), 42-60. doi:10.1108/jices-02-2018-0010
137. Smith, K.T., Smith, L.M. and Smith, J.L. (2011), "Case studies of cybercrime and its impact on marketing activity and shareholder value", *Academy of Marketing Studies Journal*, Vol. 15 No. 2, pp. 67-81
138. Spalević, Ž. (2014). Cyber security as a global challenge of the Modern Era. *Proceedings of the 1st International Scientific Conference - Sinteza 2014*. <https://doi.org/10.15308/sinteza-2014-687-692>
139. Starks, H., & Brown Trinidad, S. (2007). Choose your method: A comparison of phenomenology, discourse analysis, and grounded theory. *Qualitative Health Research*, 17(10), 1372–1380. <https://doi.org/10.1177/1049732307307031>
140. Techopedia, 2019. Statistical Mean.. [Online] Available at: <https://www.techopedia.com/definition/26136/statistical-mean> [Accessed 14 5 2023].
141. Thaw, D. (2013). The efficacy of Cybersecurity Regulation. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2241838>
142. Tuttle, B., & Dillard, J. (2007). Beyond competition: Institutional isomorphism in U.S. accounting research. *Accounting Horizons*, 21(4), 387–409. <https://doi.org/10.2308/acch.2007.21.4.387>
143. Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109, 102387. <https://doi.org/10.1016/j.cose.2021.102387>
144. Vij, Ajay (2016, June 02). The Threat is Real: Battling Cybercrime in Banking. Finextra. Retrieved from

<https://www.finextra.com/blogposting/12685/the-threat-is-real-battling-cybercrimein-banking>

145. von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security*, 26(1), 2–9.
<https://doi.org/10.1108/ics-04-2017-0025>
146. Wang, S., Li, Z., Liu, C., Zhang, X., & Zhang, H. (2014). Training data reduction to speed up SVM training. *Applied Intelligence*, 41(2), 405–420.
<https://doi.org/10.1007/s10489-014-0524-2>
147. Warrick, D. D. (2017). What leaders need to know about organizational culture. *Business Horizons*, 60(3), 395–404.
<https://doi.org/10.1016/j.bushor.2017.01.011>
148. Wood, C. C. (2008). Information Security Policies Made Easy, Version 10. Information Shield, Inc.
149. Yin, R. K., 2018. Case study research and applications: Design and methods.. s.l.:Sage publications
150. Younus, A. M., Tarazi, R., Younis, H., & Abumandil, M. (2022a). The role of behavioural intentions in implementation of bitcoin digital currency factors in terms of usage and acceptance in New Zealand: Cyber Security and Social Influence. *ECS Transactions*, 107(1), 10847–10856.
<https://doi.org/10.1149/10701.10847ecst>
151. Yu, H., & Kim, S. (2012). SVM tutorial — classification, regression and ranking. *Handbook of Natural Computing*, 479–506.
https://doi.org/10.1007/978-3-540-92910-9_15
152. Zafran. M (2017), Lab to check cyber-attack launched, News of Bahrain, Retrieved

153. Zhang, L., Wang, X. & Du, X., 2019. Feature engineering for machine learning: A review. *Neurocomputing*, Volume 415, pp. 295-304.

Appendices

Appendix A - In-Depth Interview Questions

External Influences:

Do you believe Bahrain's government is adequately equipped to stop cyberattacks on official targets? (Abdelhamid et al., 2019)

Internal Mechanisms:

Is training program a useful tool for enhancing employee awareness of cyber threats, and what are the ways to measure the impact of training and awareness activities? (Nifakos et al., 2021)

Do you recruit, retain and maintain sufficient numbers of cybersecurity professionals in the workplace? (Blažič, 2021)

In what ways does the organization engage its employees in cybersecurity education and awareness? (Bada & Nurse, 2019)

Cybersecurity culture

What do you consider the main contributing factors in creating an effective information security culture within your institution?

Do you think top management should imbed and support the information security and create cybersecurity culture within the institution? (Alnatheer, 2012)

Cybersecurity Behavior

How is the institution guiding their employees regarding cybersecurity? (Alshaikh, 2020).

What measures can be used to determine whether security training, education, and awareness efforts have been successful in changing employees' behavior? (Alshaikh, 2020).

Appendix B: CS Questionnaire



University of Bahrain
College of Business Administration

Date: 25th December 2022

Dear Sir or Madam:

Greetings

Subject: Your participation in the Questionnaire on Cybersecurity employee behavior in Bahraini Governmental Sector

We are conducting a field study related to the subject “A study of cybersecurity behaviors of Bahraini government employees”. In order to complete this study, the work includes a field survey that has to be filled by your institution. The main aim of this survey is you as Information System/ IT manager, those who have cybersecurity job responsibilities and others IT job related employee in your institution to evaluate the factors related to cybersecurity Behavior in organizations, which mainly focus on an investigation in the Bahraini governmental sector.

The collected data and information through this questionnaire will represent one of the main sources for my research work and findings. Your response, therefore, is highly appreciated. The Questionnaire is completely anonymous. Therefore, we hope that you will feel comfortable about giving your answers as frankly as possible. All your answers will be treated in the strictest confidence and will be

used only for this study. We would therefore be thoroughly and as comprehensively as possible. The outcome of this study would depend significantly on how accurate your responses are.

Thank you very much for your anticipation and your assistance. Please feel free to contact me for any further information, assistance and clarification. Thank you for your time and assistance.

Yours faithfully,

Dr. Mourad, Associate Professor

Dr. Adel Ismail Al-Alawi, Associate Professor

Please place () at the appropriate answer:

Section One: Personal and Organizational Data

1.1 Gender: ☐ Male ☐ Female

1.2 Age: ☐ Below 30 ☐ 30-39 ☐ 40-49 ☐ 50-59 ☐ 60 and above

1.3 Marital Status: ☐ Single ☐ Married with children ☐ Married ☐ no children ☐ Other

1.4 Education Level: University Degree:

☐ BSc. ☐ MSc. ☐ PhD. ☐ Other: Specify _____

1.5 Field of study:

☐ Business ☐ Engineering ☐ Science ☐ Other: Specify _____

1.6 Your job Title:

☐ Chief Information Security Officer (CISO) ☐ Security Director

☐ Security Manager ☐ Chief Operating officer (COO)

☐ IT Manager/Director /CIO ☐ Other, Specify: _____

1.7 Which professional IT Security Certifications do you have? (You may select more than one)

☐ CompTIA Security+ ☐ CEH: Certified Ethical Hacker

☐ GSEC: SANS GIAC Security Essentials

☐ CISSP: Certified Information Systems Security

Professional ☐ CISM: Certified Information Security

Manager

☐ Other Specify: _____

1.8 Work Experience

☐ Less than one year

☐ 1-5 years

☐ 6-10 years ☐ 11-15 years

☐ 16 years and more

1.9 Number of employees in your institution

☐ Less than 100

☐ 100-199

☐ 200-299

☐ 300-399☐ 400-499☐ More than 500

1.10 Your IT department is composed of the following number of employees:

☐ Less than 5☐ 5-10☐ 10-15☐ More than 15

Please use the following scale to indicate your level of agreement (based on your judgment) by placing a tick ✓ in the appropriate response.

5	4	3	2	1
Strongly agree	Agree	Neutral	Disagree	Strongly disagree

External influences

Statements	Strongly y.	Disagr ee	Neutral	Agree	Strongly agree
1. Could Bahraini society have an impact on cybersecurity cultural backgrounds within your organization?					
2. In your opinion, do government policies and regulations have an impact on organizational cybersecurity culture?					
3. Is it necessary for top management to always know the level of cyber security adoption at other organizations?					

Organizational Mechanisms

Statements	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1. Do you think that a leader is essential for building a cybersecurity culture in the organization?					
2. Are you of the opinion that employee behavior evaluations in regards to cybersecurity are able to identify employees' strengths and weaknesses, and that this can result in a significant change in their behavior?					

3. Have you seen that employee cybersecurity behavior is significantly affected by reward and punishment?					
---	--	--	--	--	--

4. Are you convinced that establishing different formal and informal organizational channels that support or engage employees in cybersecurity has a positive impact?					
5. What do you think about the fact that different training programs and tools can significantly affect employee awareness, knowledge, and behavior regarding cybersecurity? among employees.					
6. Is it your belief that management expects positive results in employees' security behavior by allocating properly cyber security budgets?					

Cybersecurity Culture

Statements	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1. Developing a cyber-culture that integrates external collaboration with a positive internal culture that includes individual, group, and organizational characteristics is essential for achieving the desired employee cybersecurity behavior, according to you?					

2. Religious, family, and social influences play a significant role in employee beliefs and values when it comes to cybersecurity?					
3. Does your institution's management make efforts to raise security awareness among employees in various ways?					
4. The Board of Directors of your institution is not involved in cybersecurity-related activities?					
5. Is it possible to encourage employees in governmental organizations to develop their security behavior by making cybersecurity programs and a cybersecurity culture mandatory?					
6. The board of directors frequently takes no role regarding important initiatives, which include security strategy, budget, and risk assessment.					
7. At your institution, have the executives given cybersecurity a strategic priority? As an example, they allocated considerable budgets for security activities, tools, and professionals.					
8. In order to keep their knowledge current, does your top management regularly discuss cybersecurity topics as a part of their leadership team meetings and individually with cyber experts?					

9. If your institution provides teamwork among its employees, would it help them to compare notes about phishing exercises and discuss other cyber-related topics?					
10. Compared to younger employees, older adults display higher levels of awareness and proficiency with cybersecurity.					
11. Do females score lower than males for security awareness and ability in your institution?					
12. In your institution, have you noticed that employees with a similar level of awareness of cybersecurity are more likely to grasp its concepts than others without such experience?					
13. One goal of a cybersecurity organizational culture is to influence the behavior of staff with respect to complying with the official security policy.					
14. The Cyber culture of an organization can improve security behavior among employees.					

Behavioral Intention

Statements	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1. Upon completion of the cybersecurity training, did employees declare their intention to follow all policies and practices at work?					

2. Is the employee intent to follow the cybersecurity policy in order to improve the organization's cybersecurity in regard to future IT after receiving the required security training or courses from your institution?					
3. It is evident that employee attitudes, beliefs, and values have a significant effect on whether employees intend to comply with cybersecurity policy requirements?					

Cybersecurity Behavior

Statements	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1. Since the employees are Through the cybersecurity training, employees gained a deeper understanding of cybersecurity and displayed improved security behavior					
3. Many cybersecurity awareness programs fail to educate the users on why security is important and fail to motivate the users to change their behavior.					
4. Changing behavior toward security requires a broader approach to security awareness, training, and education than annual computer-based trainings.					
5. As a result of compliance, employees present more impressive cybersecurity behaviors in the organization					
6. Facilitating conditions can affect the intention to use and behavior use.					

Four: Comments

Any comments or suggestions please note them here:

THANK YOU FOR YOUR PARTICIPATING IN THIS SURVEY.

Appendix C: References of Questionnaire statements

Table A.1: References of the questionnaire statements

Factor	Source
External Influences	(Alanazi et al., 2022)
Organizational Mechanisms	(Ameen et al., 2021)
Cybersecurity Culture	(Uchendu et al., 2021)
Behavioral Intention	(Ameen et al., 2021)
Cybersecurity Behavior	(Addae et al., 2019)

Appendix D: Reviewers who judged the Questionnaire

Table A.2: Names of professors, professionals and experiences who evaluate the Questionnaire

No	Name	Job title
1	Prof. Adel Al-Alawi	University of Bahrain, College of Business Professor of Management & Information
2	Dr. Mourad Messaadia	University of Bahrain, College of Business,

ملخص الدراسة

الغرض: تركز هذه الأطروحة على دراسة تأثير ثقافة الأمن السيبراني على سلوك الموظفين، وتحديدًا في القطاع المصرفي في البحرين. ستقوم الأطروحة أيضًا بتقييم تأثير التأثيرات الخارجية والآليات الداخلية على الثقافة الأمنية. وستقوم هذه الدراسة بتحديد مدى تأثير هذه العوامل على السلوك الأمني للموظفين من خلال تحديد أكثر هذه العوامل تأثيراً وأقلها تأثيراً. علاوة على ذلك، فإن الغرض من هذه الدراسة هو التعرف على التحديات التي تواجهها المؤسسات البحرينية عند تحقيق مستوى عالٍ من ثقافة الأمن السيبراني لتعزيز السلوك الأمني للموظفين. الغرض من هذا البحث هو تزويد المنظمات بمقترحات حول كيفية تحقيق مستوى عالٍ من ثقافة الأمن السيبراني.

التصميم / المنهجية/ المنهج: استخدم البحث المنهج النوعي لاكتساب معرفة واسعة بالأدبيات السابقة وتحديد ما تقترحه الأدبيات السابقة فيما يتعلق بسؤال البحث. ومن أجل إنشاء إطار مفاهيمي لهذا البحث، استخدم الباحث المنهج النوعي، والذي تم تكييفه ليتناسب بشكل أفضل مع تحليل الأطروحة من قبل الباحث. وبالمقارنة، تم استخدام النهج الكمي للحصول على إجابات لأسئلة البحث في البحرين باستخدام أسئلة منظمة ومغلقة في مقابلات جماعية مركزة. استخدمت هذه الدراسة المنهج الاستنباطي، الذي تم اختياره بحيث يتمكن الباحث من الاستدلال من العام إلى الفريد باستخدامه. وقد تم استخدام ورقة بحثية سابقة لتطوير أسئلة المقابلة، والتي تم تعديلها لتوفير بيانات أولية شاملة. ونتيجة لذلك، تم إدخال أسئلة المقابلة في نظام إدخال البيانات عبر الإنترنت وترميزها، وتم تصميم الإجابات باستخدام مقياس ليكرت (مقياس تصنيف من خمس نقاط). شملت هذه الدراسة ١٠٨ مواطن بحريني كانوا يعملون في البحرين وقت إجراء البحث. وكان المشاركون من مختلف الأحجام التنظيمية والمستويات المهنية المختلفة داخل القطاع المصرفي. بالإضافة إلى ذلك، تم استخدام عينات عشوائية لاختيار المشاركين، وتم تحليل البيانات باستخدام مسار VCM من خلال مسار التعلم الآلي.

النتائج: وتشير النتائج إلى أن جميع العوامل المقترحة لها تأثير على ثقافة الأمن السيبراني في قطاع الحظر في البحرين، والعامل الأكثر تأثيراً هو عامل الآليات التنظيمية، في حين أن العامل الأقل تأثيراً هو عامل التأثيرات الخارجية. وقد تبين أن ثقافة الأمن السيبراني يمكن أن تؤثر على نية الموظفين في التصرف وسلوكهم في مجال الأمن السيبراني.

الكلمات الرئيسية: الأمن السيبراني، ثقافة الأمن السيبراني، الثقافة التنظيمية، الوعي الأمني، سلوك الموظفين، الخدمات المصرفية البحرينية ، التعلم الآلي، آلة دعم المتجهات (SVM).



دراسة حول سلوك الأمن السيبراني للموظفين البحرينيين في القطاع المصرفي

أطروحة مقدمة كجزء من متطلبات استكمال درجة الماجستير في (إدارة الأعمال)

إعداد

زينب جعفر عبدالله بوطريف

20190218

إشراف

د. مراد مسعدية

(أستاذ مشارك)

جامعة البحرين

مملكة البحرين

يونيو 2024م