

INFORMATION SECURITY POLICY PERCEIVED
COMPLIANCE MODEL FOR STAFF IN PALESTINE
UNIVERSITIES

BY

YOUSEF MOHAMMAD MOUSA IRIQAT

A thesis submitted in fulfilment of the requirement for the
degree of Doctor of Philosophy in Information technology

Kulliyyah of Information and Communication Technology
International Islamic University Malaysia

NOVEMBER 2020

ABSTRACT

Information security policies play a significant role in securing university information assets. There should be clear information security policies in place to ensure effective staff compliance—policy perceptibility has a positive impact on employee adherence. The focus of the research is staff compliance intention of information security policies in Palestine universities. There is a need for empirical analysis on staff perception of information security policies compliance based on the intersection and combination of factors adopted from research on multiple information security theories that could have a direct/ indirect effect on staff compliance intention. Therefore, this study seeks to understand and explore staff compliance intention of information security policies based on how they perceive several factors such as perceived sanction from general deterrence theory, perceived rewards as extrinsic motivation, perceived coping appraisal from protection motivation theory, and, information quality, information privacy and facilitating conditions perceived factors from information reinforcement. Therefore, we propose a theoretical novel model built around the perception core model and the Palestinian context. The core model constitutes the perception factors, that is, how “perceived” factors directly affect “perceived” intention to comply. Our model is suited for the Palestinian context, as it works to understand staff compliance of information security policies based on staff perception of policy focused areas and staff security education and training awareness. To significantly implement the theoretical research model, the population of the study covers a wide area of Palestine from several universities to validate and confirm the model empirically using structural equation modelling. The study research design is an empirical, quantitative, exploratory (and descriptive), in addition to the developed research instrument incorporated to achieve the research methods and objectives specifically. The study objective was achieved by carefully reviewing the most appropriate potential approaches to the problem. The researcher sought a model that could find and explain any gaps in staff perception of information security policies and model factors. Thus, a novel model was designed, validated and tested. This study made a theoretical contribution through its novel model. The use of policy focused areas made the model incorporate elements from the Palestinian context directly. This is important, as current staff perceptions of information security policies play a significant role in studying them and discussing potential future policies. In this sense, it provides a methodological contribution. Furthermore, the use of data on security education and training awareness enabled us to provide potential solutions to existing problems more effectively. Security education and training awareness programs demonstrably enhance compliance intention and unify efforts between universities and their employees to mitigate security threats from insiders, be they intentional or unintentional. This constitutes a practical contribution.

خلاصة البحث

سياسات أمنية المعلومات لها دوراً كبيراً في الحفاظ على أصول المعلومات الجامعية. لذلك ينبغي أن تكون هناك سياسات أمنية واضحة في نظم المعلومات من اجل ضمان الإمتثال الفعال للموظفين - فإدراك السياسات له أثر إيجابي على التزام الموظفين. ركز هذا البحث على ادراك الموظفين في الامتثال لسياسات أمنية المعلومات في الجامعات الفلسطينية، بناء على الحاجة إلى التحليل التجريبي على أساس التقاطع والمزج لعدد من العوامل النظرية من البحوث السابقة في أمنية المعلومات التي يمكن أن يكون لها أثر مباشر / غير مباشر على امتثال الموظفين. لذلك ، تسعى هذه الدراسة لفهم واستكشاف ادراك الموظفين في الامتثال لسياسات أمنية المعلومات، وذلك بالاعتماد على عوامل مثل ادراك العقوبة من نظرية الردع العام ، وادراك المكافآت كدافع خارجي ، وادراك تقييم المواجهة من نظرية الحماية الدافعية ، وعوامل نوعية المعلومات ، وخصوصية المعلومات وتسهيل الظروف من نظرية المعلومات التعزيزية. لذلك، يقترح هذا البحث نموذجاً نظرياً جديداً مبنياً على النموذج الأساسي للادراك مما سبق من النظريات آنفة الذكر وفي السياق الفلسطيني. ويشكل النموذج الأساسي عوامل الفهم والادراك، أي كيف تؤثر العوامل "المدركة / المفهومة" تأثيراً مباشراً على النية "المتصورة/المدركة" للإمتثال. أيضاً النموذج مناسباً للسياق الفلسطيني، حيث أنه يعمل على فهم إمتثال الموظفين لسياسات أمنية المعلومات القائمة على تصور/ ادراك الموظفين للمجالات التي تركز على السياسات والتثقيف الأمني، التوعية والتدريبية للموظفين. تمتد الجامعات الفلسطينية على جميع مناطق فلسطين، ولتنفيذ نموذج البحث النظري وللتحقق من صحة النموذج وتأكيده تجريبياً باستخدام نمذجة المعادلات المهيكلية. ولتحقيق أساليب وأهداف البحث على وجه التحديد تم تصميم اداة بحث خاصة بالدراسة مبنية على عوامل الدراسة بالاضافة الى بعض من عوامل مجالات التركيز للسياسات الامنية، والتثقيف الأمني والتوعية التدريبية. وقد تحققت أهداف الدراسة عن طريق إجراء استعراض دقيق لأنسب النهج الممكنة لمعالجة المشكلة. فوضع نموذج لاستكشاف وشرح أي ثغرات في ادراك الموظفين في الامتثال لسياسات أمنية المعلومات والعوامل النموذجية. وهكذا ، تم تصميم نموذج جديد وإقراره واختباره. قدمت هذه الدراسة مساهمة نظرية من خلال نموذجها الجديد. وبما ان تصورات الموظفين الحالية لسياسات أمنية المعلومات تلعب دوراً هاماً في دراست ومناقشة السياسات المستقبلية المحتملة، باستخدام عوامل التركيز الاساسية للحماية، لذلك قدم البحث مساهمة منهجية بدمج هذه العناصر في السياق الفلسطيني مباشرة. أيضاً، فإن استخدام البيانات المتعلقة بالسياق الفلسطيني تمكننا من توفير حلول محتملة للمشاكل القائمة على نحو أكثر فعالية. تعزز بشكل واضح برامج التثقيف الأمني والتوعية التدريبية نية الامتثال وتوحيد الجهود بين الجامعات وموظفيها للتخفيف من التهديدات الأمنية ، سواء كانت مقصودة أو غير مقصودة. ويشكل ذلك مساهمة عملية.

APPROVAL PAGE

The thesis of Yousef Mohammad Mousa Iriqat has been approved by the following:

Abd. Rahman Bin Ahlan
Supervisor

Nurul Nuha Binti Abdul Molok
Co-Supervisor

Noor Hayani Binti Abd Rahim
Co-Supervisor

Akram Zeki Khedher
Internal Examiner

Ruzaini Abdullah Arshah
External Examiner

Michael Eddie Kyobe
External Examiner

Mohamed Naqib Eishan Jan
Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Yousef Mohammad Mousa Iriqat

Signature*Yousef Iriqat*.....

Date6/11/2020.....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

**DECLARATION OF COPYRIGHT AND AFFIRMATION OF
FAIR USE OF UNPUBLISHED RESEARCH**

**INFORMATION SECURITY POLICY PERCEIVED COMPLIANCE
MODEL FOR STAFF IN PALESTINE UNIVERSITIES**

I declare that the copyright holders of this thesis are jointly owned by the student and IIUM.

Copyright © 2020 Yousef Mohammad Mousa Iriqat and International Islamic University Malaysia.
All rights reserved.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.
2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.
3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Yousef Mohammad Mousa Iriqat

Yousef Iriqat

.....

Signature

6/11/2020

.....

Date

ACKNOWLEDGEMENTS

All praise to Almighty **Allah** the most merciful most compassionate and most beneficial for giving me health, strength and patience for enabling me to pursue my studies at this stage of my life.

Gratitude is always given to the soul of my parents; peace be upon them. I wish to express my heartfelt love to my beloved family; my wife, sons and daughters, my sisters and brothers of whom have unfailingly given endless patience, love and support through the PhD journey. My utmost thanks to my brother Mahmoud for his encouragement, support and always ready to help being thousands of miles away. My appreciations for the continues support of my employer Al-Quds Open University.

Special thanks and appreciation for Dr. Nurul Nuha and Dr. Noor, my co-supervisors for their time, effort and guidance.

Of course, I would like to express my honest gratitude to my supervisor, the Deputy Dean of postgraduate studies at the Kulliyyah of Information & Communication (KICT) IIUM, **Dr. Abd. Rahman Ahlan** for providing me with a wealth of help and support during this fantastic learning journey, really this work would have never been completed without his vision and direction.

TABLE OF CONTENTS

Abstract	ii
Abstract in Arabic	iii
Approval Page.....	iv
Declaration	v
Copyright Page.....	vi
Acknowledgements	vii
Table of Contents	viii
List of Tables	xii
List of Figures	xv
List of Abbreviations	xvi
CHAPTER ONE: INTRODUCTION	1
1.1 Introduction.....	1
1.2 Research Background	2
1.2.1 Research Background in Palestine.....	4
1.3 Research Problem	5
1.4 Research Aim, Questions and Objectives.....	10
1.5 Scope and Limitation of the Research	13
1.6 Structure of the Research	13
1.7 Chapter Summary	15
CHAPTER TWO: LITERATURE REVIEW	16
2.1 Introduction.....	16
2.2 Information Security	17
2.2.1 Internal Threats	21
2.2.2 University Information Security	25
2.2.3 University Staff Awareness and Compliance	28
2.2.4 University Staff InfoSec Perception	34
2.3 Information Security Review in Palestine	38
2.3.1 Information Security Review in Palestine Universities.....	41
2.4 Information Security Policies Compliance.....	44
2.4.1 Policies, Standards and Practices.....	50
2.5 Theoretical Background.....	52
2.5.1 General Deterrence Theory.....	53
2.5.2 Protection Motivation Theory	58
2.5.3 Extrinsic Motivation (Rewards)	64
2.5.4 Information Reinforcement	66
2.5.4.1 Information Privacy	66
2.5.4.2 Information Quality	71
2.5.4.3 Facilitating Conditions	74
2.5.5 Theory of Reasoned Action/Theory of Planned Behaviour	77
2.5.6 Technology Acceptance Model	78
2.5.7 Neutralization Theory	78
2.5.8 Policy Focused Areas	80

2.5.9 Security Education and Training Awareness.....	83
2.5.10 Theoretical Research Model	87
2.6 Partial Least Squares - Structural Equation Modelling	91
2.7 Chapter Summary	95

CHAPTER THREE: RESEARCH METHODOLOGY97

3.1 Introduction.....	97
3.2 Developing Research Paradigm.....	98
3.3 Objectives Accomplishment Process.....	100
3.4 Conceptual/Hypothetical Model Development	102
3.5 Research Design (Methods and Approaches).....	109
3.6 Overview of Population	111
3.6.1 Research Sample and Data Collection.....	112
3.7 Research Instrument (Quantitative Survey).....	114
3.7.1 Demographics Part.....	115
3.7.2 Theoretical Model Factors	116
3.7.3 Policy Focused Area	122
3.7.4 Staff Awareness of InfoSec Policies.....	124
3.7.5 Staff Security Education and Training Awareness	126
3.8 Research Instrument Content and Face Validity	126
3.9 Pilot Study	128
3.10 Chapter Summary	130

CHAPTER FOUR: DESCRIPTIVE DATA ANALYSIS131

4.1 Introduction.....	131
4.2 The DataSet Structure.....	132
4.3 Respondent Demographic Data Analysis	133
4.4 Policy Focused Area Analysis	138
4.4.1 Clean Disk Policy	139
4.4.2 Password Policy	141
4.4.3 Internet Usage Policy.....	143
4.4.4 Email Usage Policy.....	146
4.5 Staff Awareness of InfoSec Policies.....	150
4.6 Model Factors Descriptive Analysis.....	152
4.6.1 Perceived Sanctions	153
4.6.1.1 Perceived Sanction Certainty.....	153
4.6.1.2 Perceived Sanctions Severity.....	155
4.6.2 Perceived Rewards.....	158
4.6.3 Perceived Coping Appraisal	160
4.6.3.1 Perceived Self-Efficacy	160
4.6.3.2 Perceived Response Efficacy.....	162
4.6.4 Perceived Information Reinforcement.....	165
4.6.4.1 Perceived Information Quality	165
4.6.4.2 Perceived Information Privacy	167
4.6.4.3 Perceived Facilitating Conditions.....	169
4.6.5 Perceived Intention to Comply	172
4.7 Staff Security Education and Training Awareness	174
4.8 Chapter Summary	178

CHAPTER FIVE: STRUCTURAL MODEL ANALYSIS	180
5.1 Introduction.....	180
5.2 Measurement Model Analysis	182
5.2.1 Assessing Univariate and Multivariate Normality	183
5.2.2 Indicator Reliability	184
5.2.3 Scale Reliability: Cronbach’s Alpha and Rho_A	187
5.2.4 Composite Reliability	188
5.2.5 Convergent Reliability.....	190
5.2.6 Discriminant Validity (Vertical Collinearity).....	191
5.2.7 Common-Method Variance	194
5.3 Structural Model Analysis	195
5.3.1 Inner Path Model: Bootstrapping Resampling	197
5.3.2 Path Coefficients (β): Strength of Relationship Between Latent Constructs	198
5.3.3 Coefficient Determinations (R^2)	199
5.3.4 Path Relationship Significance	199
5.3.5 Stone-Giesser Criterion (Q^2) for Cross-Validation.....	200
5.3.6 Hypothesis Testing: Bootstrapping Direct Effect.....	201
5.4 Chapter Summary	203
 CHAPTER SIX: RESULT AND DISCUSSION	 207
6.1 Introduction.....	207
6.2 Discussion.....	208
6.2.1 Perception Research Model	208
6.2.1.1 Perceived Sanctions	209
6.2.1.2 Perceived Rewards.....	211
6.2.1.3 Perceived Coping Appraisal	212
6.2.1.4 Perceived Information Reinforcement.....	213
6.2.2 Palestine Context Factors	216
6.2.2.1 Perceived Policy Focused Areas.....	217
6.2.2.2 Staff Security Education and Training Awareness.....	219
6.2.2.3 Staff Awareness of InfoSec Policies.....	220
6.2.3 Staff Profile Difference.....	221
6.2.3.1 Staff Profiles of Perception Factors	222
6.2.3.2 Staff Profiles of Policy Focused Areas	224
6.2.3.3 Staff Profiles of SETA.....	225
6.2.4 The Final Model Result	226
6.3 Chapter Summary	227
 CHAPTER SEVEN: CONCLUSION	 228
7.1 Introduction.....	228
7.2 Conclusion	228
7.3 Research Contribution	230
7.4 Further Work and Limitation.....	232
 REFERENCES.....	 234
 APPENDIX A: THE RESEARCH INSTRUMENT	 256
APPENDIX B: PILOT STUDY RESULTS SUMMARY	266

APPENDIX C: SECOND PAPER RESULTS SUMMARY.....	268
APPENDIX D: SPSS RESULTS OUTPUT.....	269
APPENDIX E: SEM ANALYSIS RESULTS.....	271
PUBLICATIONS.....	276

LIST OF TABLES

<u>Table No.</u>		<u>Page No.</u>
2.1	Perceived Causes of Human Error	49
2.2	Policy Focused Areas Found in Other Research Summary	83
2.3	Reviewed Theories and Factors Summary	88
3.1	Comparison of paradigms between Epistemology and Ontology Stance	100
3.2	Collected Datasets from Palestine Universities	113
3.3	Measurement Variables of Perceived Sanctions	116
3.4	Measurement Variables of Perceived Rewards	118
3.5	Measurement Variables of Perceived Coping Appraisal	118
3.6	Measurement variables of Perceived Information Reinforcement	120
3.7	Measurement Variables of Perceived Intention to Comply	122
3.8	Measurement Variables of Perceived Policy Focused Areas	123
3.9	Measurement variables of Staff Awareness of InfoSec Policies	125
3.10	Measurement Variables of SETA	126
4.1	Palestine Universities Legend	132
4.2	Universities Vs Affairs Crosstabulation	134
4.3	Participants Response Bias	135
4.4	Education, Age Group and Current Job Experience Percentages	136
4.5	Crosstabulation Education Level Vs Affairs	137
4.6	Clean Desk Policy Descriptive Analysis	139
4.7	Clean disk Policy Vs Staff Profile Crosstabulation	140
4.8	Password Policy Descriptive Analysis	142
4.9	Password Policy Vs Staff Profile Crosstabulation	142

4.10	Internet Usage Policy Descriptive Analysis	144
4.11	Internet Usage Policy Vs Staff Profile Crosstabulation	145
4.12	Email Usage Policy Descriptive Analysis	147
4.13	Email Usage Policy Vs Staff Profile Crosstabulation	147
4.14	Staff Awareness of InfoSec Policies Descriptive Analysis	150
4.15	InfoSec Policies Awareness Vs Staff Profile Crosstabulation	151
4.16	Perceived Sanction Certainty Descriptive Analysis	153
4.17	Perceived Sanction Certainty Vs Staff Profile Crosstabulation	154
4.18	Perceived Sanction Severity Descriptive Analysis	156
4.19	Perceived Sanction Severity Vs Staff Profile Crosstabulation	157
4.20	Perceived Rewards Descriptive Analysis	158
4.21	Perceived Rewards Vs Staff Profile Crosstabulation	159
4.22	Perceived Self-Efficacy Descriptive Analysis	160
4.23	Perceived Self-Efficacy Vs Staff Profile Crosstabulation	161
4.24	Perceived Response Efficacy Descriptive Analysis	163
4.25	Perceived Response-Efficacy Vs Staff Profile Crosstabulation	164
4.26	Perceived Info-quality Descriptive Analysis	165
4.27	Perceived Info-Quality Vs Demographic Variable Crosstabulation	166
4.28	Perceived Info-Privacy Descriptive Analysis	167
4.29	Perceived Info-Privacy Vs Staff Profile Tabulation	168
4.30	Perceived Facilitating Conditions Descriptive Analysis	170
4.31	Perceived Facilitating Condition Vs Staff Profile Crosstabulation	171
4.32	Perceived Intention to Comply Descriptive Analysis	172
4.33	Perceived Intention to Comply Vs Staff Profile Crosstabulation	173
4.34	SETA Descriptive Results	175
4.35	SETA Vs Staff Profile Crosstabulation	177

5.1	Normality Tests	183
5.2	Outer Indicators Loadings	186
5.3	Measurement Model Reliability Scores	191
5.4	Discriminant Validity (Fornell and Larcker Criterion)	192
5.5	HTMT Results	193
5.6	Path Coefficient Strengths (β)	198
5.7	Coefficient Determinations of the Constructs	199
5.8	Significance of Path Coefficient	199
5.9	Stone-Giesser Criterion (Q^2)	201
5.10	Hypotheses Summarized Results	202

LIST OF FIGURES

<u>Figure No.</u>		<u>Page No.</u>
1.1	Major Steps to Achieve Objectives	12
2.1	General Theoretical Model	90
3.1	Objectives Accomplishment Process	101
3.2	Conceptual/Hypothesis Model; Staff Perceptions of InfoSec Policy Compliance	107
4.1	University Staff Participants by Paper or Google Form	132
4.2	Faculties, Affairs and Gender Respondent Percentages	133
4.3	Participant Education, Age group and Current Job Experience Charts	136
4.4	Overall Staff Perception of PFA Chart	149
5.1	Mardia's Multivariate Skewness and Kurtosis Tests	184
5.2	Path Model with Contributing Indicators	185
5.3	Scale reliability: Cronbach's Alpha and Rho_A	188
5.4	Composite Reliability	189
5.5	Convergent Reliability (AVE)	190
5.6	Structural Model Path Diagram	197
5.7	The Novel Contribution Model	203
6.1	Hypothetical Model Summary	208
6.2	PFA's Items Percentages Charts	217
6.3	Overall Average Percentage of SETA	219
6.4	Perception Constructs Overall Percentages	223
6.5	Significant Results of Perception Factors Vs Staff Profiles	224
6.6	Significant Results of PFA Vs Staff Profile	225

LIST OF ABBREVIATIONS

AC	Academic Staff	IRIQ	IR Info Quality
AD	Administrative Staff	ISO	International Standards Organization
ANOVA	Analysis of Variance	ISP	Information Security Policy
ASC	Staff Awareness of InfoSec Policies	ISSP	Issue-Specific Security Policies
AVE	Average Variance Extracted	IT	Information Technology
CA	Cronbach's Alpha	IUP	Internet Usage Policy
CARE	Coping Appraisal Response Efficacy	KW	Kruskal- Wallis
CASE	Coping Appraisal Self-Efficacy	NIST	National Institute of Standards and Technology
CB	Covariance-Based	NSD	Non-Statistical Difference
CDP	Clean Desk Policy	PEP	Palestine Economy Portal
CMB	Common Method Bias	PFA	Policy Focused Areas
CMV	Common-Method Variance	PLS	Partial Least Square
CR	Composite Reliability	PMT	Protection Motivation Theory
EISP	Enterprise Information Security Policy	PP	Password Policy
EM	Extrinsic Motivation	RO	Research Objective
EUP	Email Usage Policy	RQ	Research Question
GASSP	Generally Accepted Security System Principles	Rwds	Rewards
GCI	Global Cybersecurity Index	SC	Sanction Certainty
GDPR	General Data Protection Regulation	SCT	Social Cognitive Theory
GDT	General Deterrence Theory	SD	Statistical Difference
HEISC	Higher Education Information Security Council	Std.	Standard Deviation
HTMT	Heterotrait-Monotrait	SEM	Structure Equation Modelling
IC	Intention to Comply	SETA	Security Education and Training Awareness
IM	Intrinsic Motivation	Sig	Significance
InfoSec	Information Security	SS	Sanction Severity
IR	Information Reinforcement	SysSP	System-Specific Security Policies
IRFC	IR Facilitating Conditions	TAM	Technology Acceptance Model
IRIP	IR Info Privacy	TRA	Theory of Reasoned Action
		TPB	Theory of Planned Behaviour
		VIF	Variance Inflation Factor

CHAPTER ONE

INTRODUCTION

1.1 INTRODUCTION

Universities have recently begun to recognise that, in today's interconnected world, they must actively protect their information assets from both internal and external threats. As they constitute potential insider threats to information security (InfoSec), employees are often seen as the weakest link. Both employees and organisations must be aware of this rising challenge. Understanding staff perception of InfoSec policy compliance is critical for universities that want to leverage staff capabilities to mitigate InfoSec risks, specifically in developing countries, such as Palestine.

Recent studies have addressed the increasing importance of modern computer systems and information management by universities in Palestine. The widespread availability of the internet, which now extends beyond its traditional boundaries, has resulted in a wide variety of undesirable activities. As such, InfoSec policy compliance has emerged as a significant issue (ISACA, 2006; Saheb, 2013; Abdelwahed et al., 2017; Flores & Sun, 2018; Tsohou et al., 2015).

The protection of information assets and resources is critical to the proper functioning of a university. Issues such as unauthorised grade changes and persistent problems with registration or financial systems can undermine institutional credibility and viability.

Thus, more effort must be directed toward motivating staff to be security compliant and in line with university InfoSec policies (Al-Alawi et al., 2016). Universities tend to suffer from staff members who do not fulfil their InfoSec

responsibilities (Siponen et al., 2014; Silvius et al., 2012). Universities view information as one of their most valuable assets. The university environment makes for a unique dynamic in which information is constantly being exchanged, generated and applied in ways that allow affiliated students and staff on and off the campus to work with it through e-learning and shared resources (Dahbur et al., 2012).

1.2 RESEARCH BACKGROUND

Information technology is distributed around the world, meaning threats can come from anywhere through connected networks or shared resources (Sadowsky et al., 2003). According to Sadowsky et al. (2003), “Developing countries should regard InfoSec as a top priority, for the opportunity costs of not doing so may be very high indeed and criminal activity will migrate to places where controls are poor, and InfoSec is weak”.

The principles of InfoSec are the same in both developed and developing countries. However, the significance of InfoSec penetration in developing countries could be far more severe (Sadowsky et al., 2003). Developing countries often suffer from a lack of technical resources and awareness. Moreover, some developing countries may not view InfoSec as a high priority because they face many other challenges. Palestine, for instance, faces financial, political and security issues on top of the Israeli occupation.

Like other institutions, universities face both external and internal threats (Barzak et al., 2016). Internal threats can emerge from staff with direct or indirect access to information systems. Most research views internal threats as related to noncompliance behaviour and divides internal threats into *intentional* and *unintentional* (Greitzer et al., 2014; Aurigemma & Mattson, 2017; Al-Omari et al., 2012). Intentional behaviour includes actions such as information theft and deliberate ignorance of rules.

Greitzer et al. (2014) explain that unintentional behaviour is accidental, often through “inadequate system knowledge” or ignorance caused by a “lack of awareness and lack of training”.

Insider behaviour is expected to continue to be the most significant InfoSec threat. Despite this, organisations still fail to focus on this area (Kleeman, 2018; Bartnes, Moe & Heegaard, 2016; Ong & Chong, 2014; Montesdioca & Maçada, 2015; Posey, Roberts & Lowry, 2015). Employee maliciousness, negligence and human error accounted for 54% of all InfoSec incidents in 2014 (Ponemon Institute, 2016).

Staff actions, be they intentional or unintentional, can jeopardise information systems and threaten university information assets (Siponen et al., 2014; Kruger & Kearney, 2006; Flores & Sun, 2018). Several critical InfoSec operations are still not able to be fully automated, even with highly advanced technology (Silvius et al., 2012; Lebek et al., 2014; Theoharidou et al., 2005). As a result, careless behaviour among staff members, such as opening spam email links or downloading attachments from unknown emails, continues to be a significant factor for InfoSec policy violations.

InfoSec policies play a significant role in securing university information assets. There should be clear InfoSec policies in place to ensure effective staff compliance—policy visibility has a positive impact on employee adherence (Siponen et al., 2009).

Emphasising these InfoSec policies is important, as it focuses attention on security and makes staff conscious about the skills they need to protect information assets (Pérez-González, 2019; Chan et al., 2005; Muhire, 2012; Herath & Rao, 2009). Of course, staff members must have good intentions for compliance encouragement to have much of an impact (Bulgurcu et al., 2010; D’Arcy & Herath, 2011; Herath & Rao, 2009; Alshare et al., 2018).

Therefore, this study seeks to analyse the perception of “intention to comply” with InfoSec policies among university staff.

1.2.1 Research Background in Palestine.

According to Symantec, a cybersecurity firm, more than two-thirds of the organisation in the Middle East were incapable of protecting themselves from sophisticated cyber-attacks. The state of InfoSec in Palestine does not stray from that of its region; it has been negatively affected by factors such as user base growth, low security awareness, lack of law enforcement training and lack of regulation (El-Guindy, 2014). Investment in information infrastructure has increased the value of e-business and created an enormous opportunity in the region. However, not all of this investment has considered the need for security solutions while developing this infrastructure (El-Guindy, 2014).

Using the Global Cybersecurity Index (2017), the researcher sees that the GCI index in Palestine is below the 33rd percentile; only three of 25 indicators are above the 65th percentile (cybercriminal legislation, government certification and international participation). A clear gap exists between developing countries in terms of awareness, understanding and knowledge on InfoSec practices.

The Palestine Economy Portal (2016) recommends extensive reforms to the rules and regulations surrounding government and institutional InfoSec policies. PEP (2016) argues for laws and legislation to facilitate the protection and security of information; it sees this as an urgent necessity to prevent the risks of cybercrime and InfoSec threats (PEP, 2016).

Recently, there has been a rising number of publications focused on cybercrime and InfoSec in Palestine (Abdelwahed et al., 2017; Amro, 2018; Al-Saheb, 2013). According to Amro (2018), the majority of people in Palestine are connected to the

internet and generally affected by technology. However, knowledge on cybercrime, including identity theft, financial fraud and defamation, does not match up with the high level of connection. In Palestine, for example, cybercrime laws and regulations are weak and must be reviewed (Amro, 2018).

Researchers have, in recent years, showing an increased interest in Palestinian university InfoSec policies (Abdelwahed et al., 2017; Al-Saheb, 2013). Al-Saheb (2013) recommends the establishment of university-level InfoSec units and the formalisation of InfoSec policy documents to avoid the risk of cybercrimes or penetration into the university information system.

According to a recent study on Palestinian universities in Gaza by Abdelwahed et al. (2017), universities should support the InfoSec policies from the process of risk assessment and creation of InfoSec policies to the process of continually reviewing and updating InfoSec policies.

1.3 RESEARCH PROBLEM

According to Abed et al. (2016), D'Arcy & Herath (2011), Alshare et al. (2018), Pahnla et al., (2007) and Aurigemma & Mattson (2017), human (staff) perception is crucial in an efficient InfoSec environment—technical solutions are insufficient. As knowledge accumulates on InfoSec policy compliance, it initiates changes in attitude, motivation and perception that gradually initiate positive changes in staff intention (Pérez-González, 2019; Alshaikh, et al., 2018; Kleeman, 2018).

According to Siponen and Vance (2010), Herath and Rao (2009), Siponen et al. (2014) and Safa et al. (2016), the mere implementation of InfoSec policies does not guarantee that employees will comply to its provisions. Correspondingly, employees may not perceive the effectiveness and importance of protecting information assets

through InfoSec policy compliance to be high; many employees may intentionally or unintentionally ignore, resist or abandon the policies, while some may perceive it as an obstruction to them completing their tasks.

Numerous research initiatives (da Veiga et al., 2020; Lebek et al., 2014; Aurigemma & Mattson, 2017; Siponen et al., 2010; Theoharidou et al., 2005; Tsohou et al., 2015) on InfoSec behaviour and awareness have focused on theory verification and validation or have simply been literature reviews of theory comparisons used in InfoSec or InfoSec policy compliance, and, as such, may present a biased viewpoint. Many researchers propose (Siponen et al., 2010; Lebek et al., 2014; D'Arcy & Herath, 2011; Alotaibi et al., 2016; Theoharidou et al., 2005) that a theoretical model without empirical evidence of employee InfoSec policy compliance does not offer any evidence to support their models.

Some research points to contradictions in the findings of other models or frameworks (Koohang et al., 2019; Rostami, Karlsson & Kolkowska, 2020; Lebek et al., 2014; Bulgurcu et al., 2010; Tsohou et al., 2015) based on the statistical results that confirm positive or negative relationships with InfoSec policy compliance. Each study sheds light on “staff intention to comply with InfoSec policy” through determinant and demographic differences. Correspondingly, the literature review reveals that perceived value of InfoSec policies and staff intention has yet to be sufficiently investigated (Bulgurcu et al., 2010; Parsons et al., 2013; Silvius et al., 2012; Chan & Mubarak, 2012).

While there is substantial research reviewing the factors that could influence InfoSec compliance intention (Tsohou et al., 2015; Siponen & Livari, 2006; Parsons et al., 2010; Harris & Furnell, 2012; Silvius et al., 2012; Yazdanmehr & Wang, 2016) that largely agrees on the importance of InfoSec policy compliance, significant issues must

still be explored. As suggested by Bulgurcu et al. (2010), an essential contribution to academic research is identifying the factors that lead to InfoSec policy compliance—several related studies indicate that there is a gap in this regard. New research could empirically test the hypothesised research models of different individuals and institutions.

Many studies (Trang & Brendel, 2019; Al-Alawi et al., 2016; Pahnla et al., 2007; Bulgurcu et al., 2010; Abdul Molok et al., 2010) confirm that the perception of social factors, such as sanctions, rewards and motivation, directly or indirectly shape staff compliance intention. Moreover, awareness of InfoSec policies can encourage compliance intention (Vance et al., 2012; Pahnla et al., 2007; Cheng et al., 2013; Barzak et al., 2016).

Therefore, combining factors from various theories could help with two issues related to the initial phenomenon of InfoSec policy compliance. First, it will help to study how staff perceive these theoretical factors as well as the differences among perception based on staff profiles. Second, it will provide an understanding of staff perceptions of the theory's factors based on its implications or effect on staff compliance intention.

Furthermore, to put this study in the context of Palestine universities, the researcher uses an investigation of several policy focused areas (PFA) adopted from SANS (2014), such as password policy, internet usage policy, email usage policy and clean desk policy (SANS, 2014) to shed more light on Palestinian staff perception of restrictive policies and ascertain the potential reaction to (or knowledge of) InfoSec policies in the future. Foremost to further study of staff security education and training awareness (SETA).

Therefore, this study adopts factors from well-known theories related to staff compliance intention, including general deterrence theory (GDT), the theory of planned behaviour (TPB), protection motivation theory (PMT) and information reinforcement (IR). These intentions are expected to eventually influence behaviour, making recognition of InfoSec policies a latent factor. Therefore, researcher seeks insight into “staff intention to comply with InfoSec policies in the context of Palestine” by targeting Palestinian university staff and combining several factors from theories that study the sanctions, rewards, coping appraisals and information reinforcement of staff perception. The researcher hopes to achieve an improved understanding of InfoSec policies in practice so the researcher can contribute to the improvement of InfoSec policies.

The proposed conceptual model integrates “perceived” factors among the staff (sanctions, rewards, coping appraisal and information reinforcement) with perceived “intention to comply” (D’Arcy & Herath, 2011; D’Arcy et al., 2009; Abed et al., 2016). The “expected” perceived practices/policies and “expected” perceived intention to comply is suitable in the context of Palestine (a non-oil-rich Gulf country) to understand staff “perception” intention and, to an extent, their perception of PFAs as tools to mitigate security threats, specifically from insiders. Most universities could have InfoSec practices implemented and distributed to their staff, as having documented and enforced InfoSec policies to govern staff intention to comply is cost-effective in terms of technical, financial and human resources. Hence, most information systems have InfoSec policies enforced through technical and practical measures.

This issue of practical measures points out that many staff members may not even realise that InfoSec policies exist or that they are experiencing fairly limited ones. Therefore, in the context of Palestinian universities, this study attempts to measure staff awareness of InfoSec policies based on staff perception of four selected PFAs. It also