ON WOMEN, CYBER-FEMINISM AND INFORMATION SECURITY: ASSESSING SECURITY THREATS BY GENDER

David Oyebisi

decool123@gmail.com

Kennedy Njenga

knjenga@uj.ac.za

Department of Applied Information Systems, University of Johannesburg.
Email

Abstract

The continued rise in information security threats has created a sustained risk to the competitiveness of businesses using computerised technology, particularly in Africa. It is posited that employees are the weakest link to the security of information systems across African businesses. The persistent affirmative campaigns in the fields of science, technology, engineering, and mathematics (STEM) has seen a steady rise of women employees entering the Information Technology (IT) industry. On one hand, this has presented new opportunities for women to play a more meaningful and significant contribution to IT in the advent of cyberfeminism. On the other hand, women now constitute great risk to the security of information systems. This emergent trend in Africa challenges the traditional paradigms where men accounted for higher percentages of sophisticated use of and threat to IT systems. The study applied the descriptive research design to describe the level of efficacy presented by women working in South African organisations. The intention was neither to formulate nor to test any hypothesis, but to use descriptive statistics to understand women's efficacy, and the potential insider threat women could pose. A total number of 155 closed-ended questionnaires were distributed to women and men working in businesses operating in South Africa. 150 responses were obtained. A computerised statistical analysis software was used to analyse data. Results show that while both women and men had a reasonable understanding of information security tenets, women were perceived to be more cautious regarding how they expressed this understanding. The work is of significance to those in business practice in Africa because of the understanding that men will no longer be seen as the primary malefactors for information security threats. The implication for this study is that as more women are encouraged to pursue STEM disciplines, they will equally become weak links to the security of information systems. It is theorised that gender will no longer be a factor in determining security threat.

Key words: Cyberfeminism, Information security, Threats, Efficacy.

Introduction

The continued rise in information security threats such as hacking, viruses, malware, and social engineering, has created a sustained risk to the competitiveness of businesses using Information Technology (IT) in Africa. Advancement in IT use by businesses in Africa, comes from investments by foreign multinationals in the continent, cross-border listings of foreign companies in local stock markets, and the rise in wireless transactions through the electronic payment of goods and services (Osabuohien & Efobi, 2012). The use of advanced IT by multinational businesses has also brought to the continent sophisticated information security threats. Aladenusi, (2018) raises the concern that information security threats such as social engineering attacks through phone calls and unsolicited emails and short message services (SMSs) are on the rise in African countries such as Nigeria. Kenya has also witnessed an increase in computer malware and virus attacks on its small and medium enterprises (SMEs) (Makumbi, Miriti & Kahonge, 2012). While South Africa has been at the forefront of generating e-Skills necessary to raise information security awareness and also to address skills gap in the IT sector (Merkofer & Murphy, 2009) it has also witnessed its fair share of information security threats (Stander, Dunnet & Rizzo, 2009; Bougaardt & Kyobe, 2011). South Africa is amongst the topmost country in Africa targeted by phishing attacks (Dlamini & Modise, 2013).

While studies have shown that information security threats could be initiated from external attacks (such as phishing, viruses, or malware), employees are potentially disastrous as well (Willison & Warkentin, 2013). Colwill, (2009) confirms this by giving a human dimension to information systems security. It has been posited that employees are the weakest link to the security of information systems across businesses (Willison & Warkentin, 2013). Insider threats are not confined to western developed countries and more recent studies have shown similar occurrences in Africa (Aston, 2016).

Security threats come from IT use and from people who are familiar with technology (Holt & Kilger, 2008). The persistent affirmative campaigns in the fields of science, technology, engineering, and mathematics (STEM) has seen a steady rise of skilled IT men and women geared towards enhancing business competitiveness in Africa. Importantly, this drive has seen more women entering an industry that was previously male dominated. On the one hand, this has presented new opportunities for women to play a more meaningful and significant contribution to IT. On the other hand, women now constitute great risk to the security of information systems.

Since decades, STEM disciplines have been male-dominated and as a consequence most information security threats were attributed to men, accounting for a higher percentage of sophisticated end-user attacks. With a greater number of skilled women entering the IT fields and playing a meaningful role in business-driven technology, and in the advent of cyberfeminism which challenges the traditional paradigms, we postulate scenarios where increasing security threats will be bound to involve and include more women who have developed efficacy and confidence in the use of IT.

Cyberfeminism is a movement that has often been seen as an insurrection of technology and systems that favoured men, and has progressively shaped women's efficacy to technology and systems that once subdued them (Wilding & Cyberfeminist International, 1998). On this account, we also postulate a time-bound growth of technically skilled women in IT, driven by an aggressive push for women to be more involved in STEM disciplines. This emergent trend in Africa challenges the traditional paradigms where men accounted for higher percentages of sophisticated use of and threat to IT systems. This work therefore examines how information security threats are now being usurped by gender roles, where men would no longer be seen as the primary malefactors for these threats.

There have been limited studies that address the role and/or involvement of women in information security threats and we feel that this work may address these shortcomings in literature. Addressing the role of women in information security and the efficacy of technology use to drive businesses especially in Africa where this study is anchored, will enable us to have a better understanding of emerging gender role and how this is now changing. This paper provides a compelling opportunity to do so. We therefore describe:

- the extent to which information security threats have been usurped by gender in the advent of skilled women entering the IT sector, and
- perceptions of information security threats by gender.

The paper is presented as follows: section one places the context of women, cyberfeminism and the extent to which there could be dissimilar efficacy in addressing security concerns; section two reviews literature concerning women and gender biases in the field of IT and specifically the role of cyberfeminism movements; section three addresses the methodology used in the work, while the penultimate and concluding sections report on data analysis and what this means to businesses.

Literature Review

Gender and Information Technology

Studies on gender role in the field of IT presents pertinent perspectives such as differences in diffusion and the underrepresentation of women in this field, (Diekman et al., 2010) the level of skills and literacy mismatch (Kim, Kil, & Shin, 2014) and career choices differentiated between gender (Gorbacheva, Craig, Beekhuyzen, & Coldwell-Neilson, 2014). For decades, the prevailing paradigm has been that IT is a male-dominated field with studies showing that boys (in high schools), believed that their IT efficacy was much higher. Often the predominant notion is the measure of competency skewed in favour of males and particularly in favour of work tasks perceived as requiring physical power to produce output (Lucas & Steimel, 2009). Recent meta-analysis, however discounts many of the above notions (Siddiq & Scherer, 2019).

Culturally, in Africa, the prevailing belief is that certain positions are the preserve of men (Dolado, Felgueroso, & Jimeno, 2003). This idea expresses itself in many academic discourses that document occupational segregation in favour of men (Stier & Yaish, 2014). A review of literature as presented in Table 1 shows the different focus areas on gender studies in the field of IT. Many of these studies, however, tend to be skewed in favour of

developed countries and underrepresent many of the gender assumptions prevailing in Africa.

Table 1: IT gender studies

Author	Context In Literature	Women In IT Career	Developing Country Context	Empowerment Context
Ray et al. (1999).	*Attempts to compare men and women's attitudes towards the value of technology, the impact of computer technology, and the comfort of using a computer.*	✓		
Jackson et al. (2001).	*Seeks to understand the differences in internet use by men and women and the factors responsible for the dissimilarities.*	✓		
Fountain, J. E. (2000).	*Seeks to understand the role women play as designers of Information Technology in the information-based society.*	✓		✓
Khreisat, L. (2009).	*Seeks to investigate women's level of education and participation in Information Technology and Computing in Jordan.*	✓	✓	✓
Ahuja, M. K. (2002).	*Seeks to address three distinct career stages of women as they make career choices in the field of Information Technology. The effects of social (e.g. work-family conflict) and structural barriers are identified.*	✓		✓
Diekman et al. (2010).	*Seeks to address the underrepresentation of women in the fields of science, technology, engineering, and mathematics (STEM).*	✓		✓
Hilbert, M. (2011).	*Attempts to compare women and men's ease of access to Information and Communication Technology and its uses thereof in developing countries.*	✓	✓	
Shirazi, F. (2012).	*Seeks to investigate the role ICT plays in liberating women in Iran in the struggle for social justice.*	✓	✓	✓
Ben Moussa, M., & Seraphim, J. (2017).	*Seeks to understand how Emirati women incorporated internet usage in their daily activity and how they take advantage of the internet to close the gap of a gender divide.*	✓		✓
Cai et al. (2017).	*Seeks to understand gender-based attitudes toward technology use through meta-analysis.*	✓		
McGee, K. (2018).	*Seeks to understand the progression of*	✓		✓

McGee, K. (2018).	*Seeks to understand the progression of Hispanic American/Latina, European American/white, Asian American and African American/black women from technical/operational IT roles to senior IT executive roles in the American corporate world.*			

A review of Table 1 suggests that few studies in developing countries address the role of IT efficacy in women. A common theme in the above studies is that globally, women are taking a proactive stance against technology and systems that once subdued them. Ray, Sormunen, and Harris's (1999) study confirms that women believe that the use of computers makes them more productive. Jackson et al. (2001) consider that while women underutilise the potential of the Internet, they are more likely to use e-mail more frequently than men. Both Fountain (2000) and Khreisat (2009) acknowledge that a significant increase in the number of women in technical roles will improve human capital deficit, and enhance procedures and standards that will benefit the society at large. According to Diekman et al., (2010) there is a notable underrepresentation of women in the fields of science, technology, engineering, and mathematics (STEM), and this has limited women's access to education, employment, and higher income (Hilbert, 2011). There has not been any clear indication that new technologies alone will change the male-dominated field of IT (Shirazi, 2012; Ben Moussa & Seraphim, 2017). Cai, Fan and Du's (2017) empirical studies however, have presented cases contrary to this regarding inconstancies on the use of technology by gender. McGee's (2018) study considers differences in ethnicity and race as contributors in determining the career progression of women.

There has been an increased involvement of African women in STEM because of aggressive campaigns and empowerment programmes (Hilbert, 2011). STEM programmes are necessary for business innovative capacity, economic development, and global competitiveness (Beede, Julian, & Langdon, et al., 2011). According to Quiros, Morales, & Pastoret, al., (2018) studies undertaken in the United States (U.S.) show that in 2013, about 15 percent of graduates in computer science were women, and 24 percent the following year. Europe has equally witnessed an increase in the educational level of entrepreneur women in IT with most self-employed women in IT being managers or professionals (Quiros et al. (2018).

With more opportunities for college and university educated women opening up in the IT industry, the more the industry will begin to realise untapped potential for progress (Beede et al., 2011). Studies have shown that women with STEM jobs have earned 33 percent more income compared to women in non-STEM jobs (Seierstad & Kirton, 2015; Vokic, Coric, & Obadic, 2017). It is a concern that women are more likely to leave their professional job than men (Fouad, Chang, Wan, & Singh, 2017) and that men are more likely to sustain jobs in IT (Kelan, 2007; Chandrasekar & Prakash, 2011; Gupta, Jain, & Vashishth, 2017).

Efficacy, the cyberfeminist and information security

Businesses driven by IT continue to report an increase in information security threats with the primary motive being personal gain (Padayachee, 2015). Information security threat

disclosures in the U.S. health industry increased between the years 2005 and 2012, where "personal identifiable data were compromised in 74 percent of the cases and personal financial data were compromised in 22 percent of the cases" (Sen & Borle, 2015, pp.316). As the percentage of women in the IT sector increases over time, it is expected that cyber malevolency will extend to this group as well. The traditional discourse as reported by Boler, Sears, & Dwight (2006) on reconstructing long held fables presents common discourses regarding women in the cyber security space as follows:

- Women are usually absent from the cyberfrontier
- Women are usually in need of protection on the cyberfrontier
- There is the invisible female teacher overshadowed by technology
- The woman teacher is deficient without technology
- Girls need to be policed (based in essentialism where males and females are believed to have dissimilar characteristics and dispositions (Burke & Singh, 2014; Vokic, Coric, & Obadic, 2017).

Plant (2000) challenges the above notions and addresses the era of the "cyberfeminist virus" (p. 265) where efficacy in women using technology offers the potential to threaten systems and reinvent gender boundaries. Indeed Plant (2000) suggests that:

"Complex systems and virtual worlds are not only important because they open spaces for existing women within an already existing culture, but also because of the extent to which they undermine both the world view and the material reality to two thousand years of patriarchal control" (pp. 265).

The cyberfeminist movement has resulted in increased efficacy in women's ability to use technology. Self-efficacy considers employees beliefs and their capacity to influence events that affect their lives (Bandura, 2010).The capacity to influence one's own life has been the core foundation of motivation and performance (Bandura, 2010).

Insider Threats

Cyberfeminism has resulted in more women acting as insider threats to organisational information systems. This was not previously the case. Past studies that had examined insider threats showed that 96 percent of the insider threats were from men (Keeney, Kowalski, Cappelli, Moore, Shimeall, & Rogers, 2005). Cappelli, Caron, Trzeciak, and Moore (2008) have shown that men were responsible for using programming techniques tools to exploit vulnerabilities present in information systems. These studies established that the threats perpetrated by men accounted for 80 percent of the confidential information being compromised. More recent studies by Kowalski, Cappelli, and Moore (2008) present a shift on the role women have played as insider threats and present results that place both men and women accounting for security threats in equal proportion. In support of this notion, Cappelli et al. (2008) found that theft of electronics asset, exploiting vulnerabilities of information systems for financial gain and fraudulent activities were perpetrated equally by both men and women.

While taking cognisance of decades of studies showing that insider employees' threats were mostly committed by men (Magklaras & Furnell, 2005), the rise of the cyberfeminist has started to challenge these assumptions. According to Hawthorne & Klein (1999);

"Cyberfeminism is a philosophy which acknowledges, firstly, that there are differences in power between women and men specifically in the digital discourse; and secondly, that cyberfeminists want to change that situation" (pp. 2).

The unintended consequence of the cyberfeminist movement (not to be confused with cyber girlism which advocates for feminist rebellion in cyber space), has been the creation of complex images of women in the cyber space (Wilding & Cyberfeminist International, 1998). Cyberfeminist have adopted strategies similar to feminism such as strategic separation of having women only mailing lists, women only self-help groups, cyber chats, networks and even women only technology training (Wilding & Cyberfeminist International, 1998). What is interesting with this group is the propensity to present efficacy in technical skills displayed by men which can serve as threats to information systems. Indeed Millar (1998) identified with this concern in defining cyberfeminism as:

"A women-centred perspective that advocates women's use of new information and communications technologies for empowerment. Some cyberfeminists see these technologies as inherently liberatory and argue that their development will lead to an end to male superiority because women are uniquely suited to life in the digital age" (pp.200).

While the use of the term cyberfeminism has faded away, it would be important to address the remnant of these ideas and how far these ideas have permeated into women in workplaces. The extent to which efficacy advocated by cyberfeminism, could potentially serve as a security risk to systems, and the extent to which some of the ideas have filtered into African businesses and to women who are increasingly playing key technical roles in these businesses, is worth considering. The section that follows presents the methodology used to elicit insights regarding efficacy by women using IT, and whether women in Africa tend to present efficacy.

Methodology

The study applied the descriptive research design to describe the level of efficacy presented by women working in South African organisations. The intention was neither to formulate nor to test any hypothesis but to use descriptive statistics to understand women's efficacy and the potential for women to become insider threats to business information systems. Descriptive research design has been used in social psychology and science as a method that helps gain a general overview of a topic of interest (Dulock, 1993). The need for descriptive research is for the development of a body of work that can be used as a pre-cursor to empirical quantitative research designs, which point to what variables would possibly be tested.

Study sample, instrument and date collection

The study sample was anchored on employees of both gender, sourced from small to medium scale enterprises (SMEs) in the Gauteng province of South Africa. A pre-sampling session was carried out with 5 participants. Results from this session enabled the researchers

to identify suitable SMEs, that were active in the field of electronic commerce, banking, tax, audit, and insurance and which relied actively on IT to carry out business activities. A total number of 155 closed-ended questionnaires were distributed to the employees in these SMEs, based on a prescribed approach suggested by Daniel (2012). 150 responses were obtained. A non-probability sampling technique which was used methodically adopted Daniel's (2012) steps in selecting a purposive sample. We intentionally targeted only those who work with IT within these businesses.

A plan was created to recruit and select technical people for elicitation of data, carefully preserving the anonymity of respondents. We were conscious that the sample did not fully represent the general profile of South Africa because it constituted intentionally selected respondents with technical proficiency. A questionnaire was developed for this purpose. The purpose and benefits of the study were outlined in the introductory sections of the questionnaire. The approximate time of completion, and ethics, and privacy issues were also addressed in the questionnaire.

Describing the data

A computerised statistical analysis software was used to generate descriptive statistics for gender. Gender was measured by dichotomous attributes where responses were coded as male = 1 and female = 0. The result shows that male participants accounted for fifty-three percent of the sample while females accounted for forty-seven percent. Figure 1 represents gender distribution of the respondents.

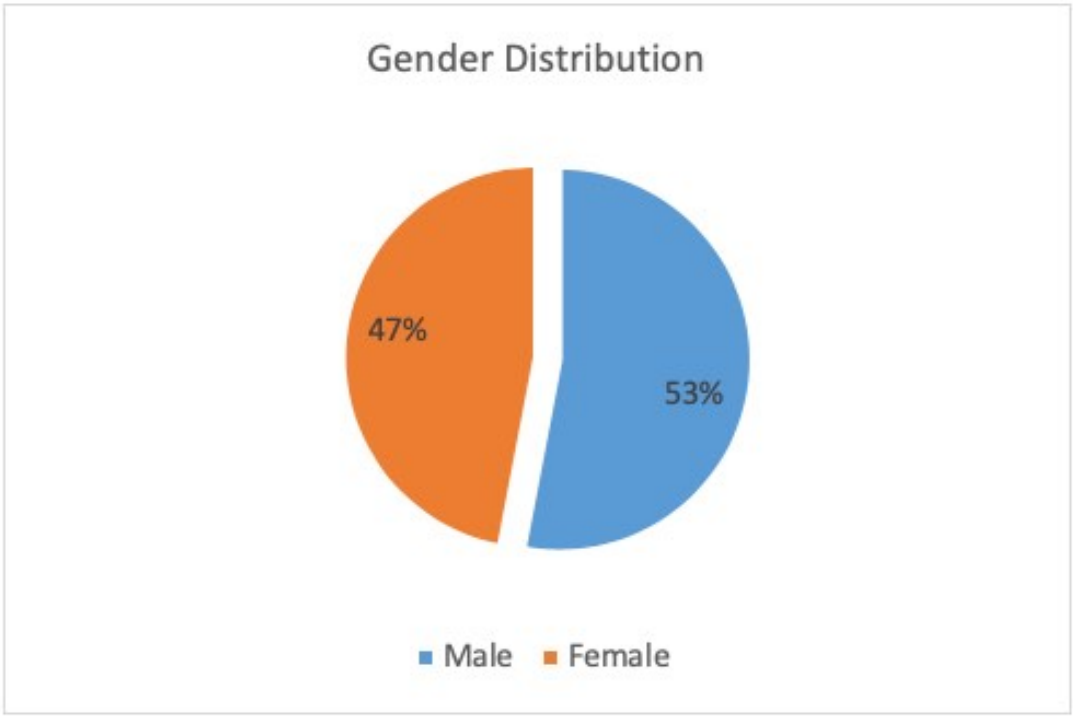

Figure 1: Gender distribution

Majority of the respondents' highest qualification was a Bachelor's degree for both men and women and shown in Table 2 (55.1% for men 38.9% for women). About a quarter of the respondents had a Master's degree (30% for men and 22% for women). Of interest was that data reveals that women Doctoral holders were proportionately more than their male colleagues.

Table 2: Qualifications

Qualifications						
Gender			**Frequency**	**Percent**	**Valid Percent**	**Cumulati Percent**
1 Male	Valid	1 Grade 12/O level or lower	1	1.3	1.3	
		2 Diploma or Certificate	9	11.5	11.5	1
		3 Bachelor's Degree	43	55.1	55.1	6
		4 Master's Degree	24	30.8	30.8	9
		5 Doctoral Degree	1	1.3	1.3	10
		Total	78	100.0	100.0	
2 Female	Valid	1 Grade 12/O level or lower	10	13.9	13.9	1
		2 Diploma or Certificate	17	23.6	23.6	3
		3 Bachelor's Degree	28	38.9	38.9	7
		4 Master's Degree	16	22.2	22.2	9
		5 Doctoral Degree	1	1.4	1.4	10
		Total	72	100.0	100.0	

From the sample taken, men were seen to have worked longer than women confirming IT literature which states that men have traditionally dominated the workplace, in particular STEM fields such as IT. Table 3 points this out as well, while also highlighting that close to 65% of the women sampled had between 2 years or less of work experience, contrasted to men sampled who had 26% of work experience, or less. This is interpreted to mean that there is an aggressive push to ensure that women are now entering these fields or a more radical view that perceives that opportunities opening up for men aren't as forthcoming as they have been traditionally.

Table 3: IT Experience

IT Experience						
Gender			Frequency	Percent	Valid Percent	Cumulative Percent
1 Male	Valid	1 Less than 1 Year	13	16.7	17.3	
		2 1-2 years	8	10.3	10.7	
		3 2-5 Years	10	12.8	13.3	
		4 5-10 years	27	34.6	36.0	
		5 10-15 years	8	10.3	10.7	
		6 15-20 years	8	10.3	10.7	
		8	1	1.3	1.3	
		Total	75	96.2	100.0	
	Missing	System	3	3.8		
	Total		78	100.0		
2 Female	Valid	1 Less than 1 Year	33	45.8	47.8	
		2 1-2 years	15	20.8	21.7	
		3 2-5 Years	12	16.7	17.4	
		4 5-10 years	7	9.7	10.1	
		5 10-15 years	1	1.4	1.4	
		6 15-20 years	1	1.4	1.4	
		Total	69	95.8	100.0	
	Missing	System	3	4.2		
	Total		72	100.0		

Analysis and Results

Gender-based security risk and efficacy

We tested efficacy by gender, and contrasted beliefs held by men and women regarding information security principles and risk by itemising 10 general constructs popular in information security literature and we carefully worded these constructs to elicit respondents' security threat efficacy. We used SPSS statistical software to generate custom tables such as the one shown by Table 4. Responses to each item range from 1 (strongly disagree) to 5 (strongly agreed). A high score (4-5) indicates a lower risk of insider threat behaviour while a lower (1-2) suggests a higher risk of insider threat and therefore threat efficacy.

Table 4: Gender-based efficacy of IT and Information Security

Item	Construct	Elicitation		Gender	
				Male	Fe
				N %	N
Item #1	Situation ethics for security	Conceptualising employee threats to the organisation as disastrous. [***Proportionally higher % of women strongly disagree, disagree, or are neutral, than men at 19% of sample size***]	Strongly disagree	0%	
			Disagree	1%	
			Neutral	6%	
			Agree	45%	
			Strongly agree	47%	
Item #2	Extra-role behaviour	Reporting and not concealing suspicious malicious behaviour of a co-worker. [***Proportionally higher % of women strongly disagree, disagree, or are neutral, than men at 20% of sample size***]	Strongly disagree	0%	
			Disagree	4%	
			Neutral	9%	
			Agree	50%	
			Strongly agree	37%	
Item #3	Information security awareness	Defining and adhering to security policies regarding the use of removable media. [***Proportionally higher % of women strongly disagree, disagree, or are neutral, than men at 33% of sample size***]	Strongly disagree	1%	
			Disagree	3%	
			Neutral	12%	
			Agree	45%	
			Strongly agree	39%	
Item #4	Protection behaviour	Prohibiting password sharing with a colleague at work. [***Proportionally higher % of women strongly disagree, disagree, or are neutral, than men at 20% of sample size***]	Strongly disagree	0%	
			Disagree	4%	
			Neutral	4%	
			Agree	32%	
			Strongly agree	60%	
Item #5	Information security configuration	Creating and authorising access to systems to discourage exploits. [***Proportionally higher % of women strongly disagree, disagree, or are neutral, than men at 11% of sample size***]	Strongly disagree	0%	
			Disagree	1%	
			Neutral	8%	
			Agree	35%	
			Strongly agree	56%	
Item #6	Threat avoidance and risk prevention	Running antivirus check on removable media (USB) prior to use. [***Proportionally higher % of women strongly disagree, disagree, or are neutral, than men at 8% of sample size***]	Strongly disagree	0%	
			Disagree	0%	
			Neutral	4%	
			Agree	40%	
			Strongly agree	56%	
Item #7	Employee security awareness	Discerning pirated software as harmful to systems. [***Proportionally higher % of women strongly disagree, disagree, or are neutral, than men at 16% of sample size***]	Strongly disagree	1%	
			Disagree	3%	
			Neutral	3%	
			Agree	41%	
			Strongly agree	53%	
Item #8	Privacy policy efficacy	Initiating need to lock computer screens during short breaks. [***Proportionally higher % of women strongly disagree, disagree, or are neutral, than men at 15% of sample size***]	Strongly disagree	1%	
			Disagree	1%	
			Neutral	6%	
			Agree	46%	
			Strongly agree	45%	
Item #9	Security risk and benefit trade-off	Discourage downloading unsolicited but interesting attachments. [***Proportionally higher % of women strongly disagree, disagree, or are neutral, than men at 12% of sample size***]	Strongly disagree	0%	
			Disagree	1%	
			Neutral	9%	
			Agree	40%	
			Strongly agree	50%	
Item #10	Security and Privacy balance	Discourage deactivating computer protective software if the network is slow. [***Proportionally higher % of women strongly disagree, disagree, or are neutral, than men at 21% of sample size***]	Strongly disagree	0%	
			Disagree	3%	
			Neutral	12%	
			Agree	37%	
			Strongly agree	49%	

Table 4 presents some very interesting insights. While all respondents strongly agreed with all the 10 constructs meant to establish strong mechanisms for businesses to protect systems from threats (insider threats) which was what we expected, what we realised was that women proportionally disagreed with all these tenets in greater proportion to men. We found this very compelling and we interpret this to mean that perhaps the shift and digital discourse presented in Hawthorne & Klein's (1999) work is slowly expressing and

presenting itself through women in African workplaces. We further investigated this difference in efficacy and security perspective by carrying out a normality test which is explained in the next section.

Discussions

The protection of business information assets is a crucial behavioural trait requiring employees to be aware of security risk and to contemplate extra-role and protection behaviour as concise choices. The fact that data analysis presented dissimilar efficacy and perspectives between the choices made by gender could be troubling to organisations, because of the inconsistency presented by gender with regard to matters of information security. What is more concerning is that females were inclined to be less concise (many selecting neutral) on information security issues deemed important. We consider this as an information security risk in its own right. We categorised the top 3 concerns where more women were indecisive or disagreed with these constructs in higher proportion to men, as presented in Table 5, and offer a proposition on how this can be addressed.

Table 5: Independent Samples Test table for male and female group

Ranking of Item **Top 3 items**		**Proportion of women strongly disagree, disagree or are neutral to constructs**	**Construct**	**Corporate Propositio to include women security issues.**
1	Item #3	33%	Information security awareness	*Technology is not Subjugation*
2	Item #10	21%	Security and Privacy balance	*Mentorship*
3	Item #2, Item #4	20%	Extra-role behaviour, Protection behaviour	*Shaping and defining career paths to assist i behaviour*

Technology is not Subjugation

In order to close the gap in security awareness, women should be made comfortable with technology and not see technology, as a way of subjugation (as sometimes prescribed in the older ideals of cyberfeminism).

Mentorship

Businesses should establish mentoring programmes for women by women, for better understanding of the balance between security and privacy. Cyberfeminism addresses the issue regarding well informed women with technical skills helping shape and guide positively, less experienced women, to navigate the cyber security and information security space.

Shaping and defining career paths to assist in behaviour

Businesses should identify gaps on career growth for women in the cyber security space by establishing clear paths that address not only low participation but participation, that yields less security risks to corporate assets as this study has shown is likely to happen.

Implication to Practice

This study undoubtedly raises a growing concern that both genders have a critical role to play regarding the security of information held in business systems. In the light of issues raised in section 4.1, 4.2 and 4.3 respectively, we believe businesses can benefit by expanding female participation in the cyber security space through training and employment programs, mentorship and of raising awareness regarding security risk. The study highlights that if participation is not managed carefully, then the chances that either gender becomes a malefactor to security threats are heightened.

Limitation of study and future research

This study research has limitations that present fresh and novel possibilities for important future research. Firstly, our results of the descriptive research may not in any way be used to provide a definitive answer regarding the efficacy of women and their potential to become insider threats to an organisation. It may not do so since the work has neither proved nor disproved any hypothesis. However having in mind this limitation, the descriptive research was seen as a useful tool in this and in many other areas of scientific research, where descriptive research design has been used. Since the descriptions are without hard quantitative rules, there could have been a number of ways to determine efficacy. However, we made effort to provide rigour in describing quantitative data obtained by assessing women's predisposition for efficacy as provided in Table 4. Nevertheless, future research should further substantiate specific hypotheses and empirically test the hypotheses through scrutiny. Also, data was obtained from 150 respondents. Future studies would need to extend this sample.

Conclusion

We place this study not as one that proposed to defy the important ideals of women and cyberfeminism on the use of technology, but rather one that is important in addressing the difference in gender perspective regarding information security. While we may acknowledge that some of the ideals held by these movements may have embraced and even influenced, the responses females gave to this study, the scope of this work was limited to the differences in efficacy regarding security threats. Perhaps further work would consider looking into the extent to which feminists' movements may have influenced information and cyber security. Our work primarily addresses an important concern: namely, that efficacy towards information security particularly from women presented concerns to businesses and that such efficacy manifested differently in men. Indeed, information security threats are now being usurped by gender roles, in that men are no longer seen as the primary malefactors for these security threats. Although females are generally believed to be less prone to committing insider attack, as compared to their male counterparts, our research finding has discovered a new trend in this development. We consider such discernments as worrying to organisations. Our work has made propositions regarding what businesses could do about this. We hope

that this work placed in the context of businesses operating in Africa presents exciting and useful insights that would shape how African businesses operate in the future.

References

Ahuja, M. (2002). Women in the information technology profession: A literature review, synthesis and research agenda. European Journal of Information Systems, 11(1), 20-34. doi:10.1057/palgrave/ejis/3000417

Aladenusi, T. (2018). 2018 Nigeria Cybersecurity Outlook. Retrieved from https://www2.deloitte.com/ng/en/pages/risk/articles/2018_nigeria_cybersecurity_outlook.html

Aston, G. (2016). Can you beat the data thieves? H&HN Hospitals & Health Networks, 90(2), 20-25.

Bandura, A. (2010). Self-efficacy. The Corsini encyclopedia of psychology, 1-3.

Ben Moussa, M., & Seraphim, J. (2017). Digital gender divides and E-empowerment in the UAE: A critical perspective. International Journal of Education and Development using Information and Communication Technology, 13(3), 145-161.

Beede, D. N., Julian, T. A., Langdon, D., McKittrick, G., Khan, B., & Doms, M. E. (2011). Women in STEM: A gender gap to innovation. Economics and Statistics Administration Issue Brief, (04-11).

Boler, M., Sears, P., & Dwight, J. S. (2006). Reconstructing the Fables: Women on the Educational Cyberfrontier. In The International Handbook of Virtual Learning Environments (pp. 1467-1494). Springer, Dordrecht.

Bougaardt, G., & Kyobe, M. (2011). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa. In ICIME 2011-Proceedings of the 2nd International Conference on Information Management and Evaluation: ICIME 2011 Ryerson University, Toronto, Canada, 27-28 April 2011 (p. 62). Academic Conferences Limited.

Burke, R. J., & Singh, P. (2014). Correlates of career priority and family priority among hospital-based nursing staff. Gender in Management, 29(2), 91-107. doi:10.1108/GM-05-2013-0050

Cai, Z., Fan, X., & Du, J. (2017). Gender and attitudes toward technology use: A meta-analysis. Computers & Education, 105, 1-13. doi:10.1016/j.compedu.2016.11.003

Cappelli, D., T. Caron, R. Trzeciak, & A. Moore. (2008). Spotlight On: Programming Techniques Used as an Insider Attack Tool.

Chandrasekar, K.S. & Siva Prakash, C.S. (2011). Women Empowerment ICT Enterprises, SCMS Journal of Indian Management, 8(1), 18-27.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days?. Information security technical report, 14(4), 186-196.

Daniel, J. (2012). Sampling essentials: Practical guidelines for making sampling choices. Los Angeles: Sage.

Dlamini, Z., & Modise, M. (2013). Cyber security awareness initiatives in South Africa: a synergy approach. Case Stud. Inf. Warf. Secur. Res. Teach. Stud, 1.

Diekman, A. B., Brown, E. R., Johnston, A. M., & Clark, E. K. (2010). Seeking congruity between goals and roles: A new look at why women opt out of science, technology, engineering, and mathematics careers. Psychological Science, 21(8), 1051. doi:10.1177/0956797610377342

Dolado, J. J., Felgueroso, F., & Jimeno, J. F. (2003). Where do women work?: Analysing patterns in occupational segregation by gender. Annales d'Economie Et De Statistique, (71-72), 293-315. doi: 10.2307 / 20079056

Dulock, H., (1993). Research Design: Descriptive Research, Journal of Paediatric Oncology Nursing Vol 10, 154-157.

Fouad, N. A., Chang, W. H., Wan, M., & Singh, R. (2017). Women's Reasons for Leaving the Engineering Field. Frontiers in psychology, 8, 875. doi:10.3389/fpsyg.2017.00875

Fountain, J. E. (2000). Constructing the information society: Women, information technology, and design doi:https://0-doi-org.ujlink.uj.ac.za/10.1016/S0160-791X(99)00036-6

Gorbacheva, E., Craig, A., Beekhuyzen, J., Coldwell-Neilson, J. (2014). ICT interventions for girls: Factors influencing ICT career intentions. Australasian Journal of Information Systems, 18(3) doi:10.3127/ajis.v18i3.1103

Gupta, P., Jain, S. & Vashishth, N. (2017). E-Governance in India: A Case Study of Leveraging Information & Communication Technology (ICT) for Women Empowerment under MGNREGA in the State of Rajasthan, Journal of Governance & Public Policy, 7(1), 78-87.

Hawthorne, S., & Klein, R. (Eds.). (1999). Cyberfeminism: Connectivity, critique and creativity. Spinifex Press.

Hilbert, M. (2011). Digital gender divide or technologically empowered women in developing countries? A typical case of lies, damned lies, and statistics doi:https://0-doi-org.ujlink.uj.ac.za/10.1016/j.wsif.2011.07.001

Holt, T. J., & Kilger, M. (2008). Techcrafters and makecrafters: A comparison of two populations of hackers. In 2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing (pp. 67-78). IEEE.

Jackson, L., Ervin, K., Gardner, P., & Schmitt, N. (2001). Gender and the internet: Women communicating and men searching. Sex Roles, 44(5-6), 363-379.

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T. & Rogers, S. (2005). Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. CERT

Program and Software Engineering Institute. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a636653.pdf

Kelan, E. K. (2007). 'I don't know why' - accounting for the scarcity of women in ICT work. Women's Studies International Forum, 30(6), 499. doi:10.1016/j.wsif.2007.09.003

Khreisat, L. (2009). The under-representation of women in information technology and computing in the middle east: A perspective from jordan doi: https://doi.org/10.1016/j.techsoc.2009.06.006

Kim, H., Kil, H., & Shin, A. (2014). An analysis of variables affecting the ICT literacy level of korean elementary school students. Computers & Education, 77, 29-38. doi:10.1016/j.compedu.2014.04.009

Kowalski, E., D. Cappelli, &. Moore, A. (2008). Insider Threat Study: Illicit Cyber Activity in the Information Technology and Telecommunications Sector. Software Engineering Institute, Carnegie University, Retrieved from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52257

Lucas, K., & Steimel, S. J. (2009). Creating and responding to the gen(d)eralized other: Women miners' community-constructed identities. Women's Studies in Communication, 32(3), 320. doi:10.1080/07491409.2009.10162393

Magklaras, G. B., & Furnell, S. M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. Computers and Security, 24(5), 371. doi:10.1016/j.cose.2004.10.003

McGee, K. (2018). The influence of gender, and race/ethnicity on advancement in information technology (IT) doi:https://0-doi-org.ujlink.uj.ac.za/10.1016/j.infoandorg.2017.12.001

Merkofer, P., & Murphy, A. (2009). The e-skills landscape in South Africa. Zeitschrift für Politikberatung, 2(4), 685-695.

Makumbi, L., Miriti, E. K., & Kahonge, A. M. (2012). An Analysis of information technology (IT) security practices: A case study of Kenyan small and medium enterprises (SMEs) in the financial sector. International Journal of Computer Applications, 57(18).

Millar, M. S. (1998). Cracking the gender code: Who rules the wired world?. Canadian Scholars' Press.

Osabuohien, E. S., & Efobi, U. R. (2012). Technology diffusion and economic progress in Africa: Challenges and opportunities. In Disruptive technologies, innovation and global redesign: Emerging implications (pp. 425-440). IGI Global.

Padayachee, K. (2015). An insider threat neutralisation mitigation model predicated on cognitive dissonance (ITNMCD). South African Computer Journal, 56(1), 50-79.

Pallant, J. (2016). SPSS survival manual: a step by step guide to data analysis using IBM SPSS, Sixth edn, Allen & Unwin, Sydney.

Plant, S. (2000). On the matrix: Cyberfeminist simulations. The cybercultures reader, 325-336.

Quiros, C.T., Morales, E.G., Pastor, R.R., Carmona, A.F., Ibanez, M.S., & Herrera, U.M. (2018). Women in the Digital Age. Retrieved from http://www.media2000.it/wp-content/uploads/2018/03/WomeninDigitalAgeStudy-FinalReport.pdf

Ray, C. M., Sormunen, M., & Harris, T. M. (1999). Men's and women's attitudes toward computer technology: A comparison. Information Technology, Learning, and Performance Journal, 17(1), 1-8.

Seierstad, C. & Kirton, G. (2015). Having it all? women in high commitment careers and work-life balance in norway. Gender, Work and Organization, 22(4), 390. doi:10.1111/gwao.12099

Sen, R., & Borle, S. (2015) Estimating the contextual risk of data breach: An empirical approach. Journal of Management Information Systems, 32(2), 314. doi:10.1080/07421222.2015.1063315

Shirazi, F. (2012). Information and communication technology and women empowerment in iran. Telematics and Informatics, 29(1), 45-55. doi:10.1016/j.tele.2011.02.001

Siddiq, F., & Scherer, R. (2019). Is there a gender gap? A meta-analysis of the gender differences in students' ICT literacy. Educational Research Review, doi:10.1016/j.edurev.2019.03.007

Stander, A., Dunnet, A., & Rizzo, J. (2009). A Survey of Computer Crime and Security in South Africa. In ISSA (pp. 217-226).

Stier, H. & Yaish, M. (2014). Occupational segregation and gender inequality in job quality: A multi-level approach. Work, Employment and Society, 28(2), 225. doi:10.1177/0950017013510758

Vokic, N.P., Coric, D.S. & Obadic, A. (2017). To be or not to be a woman? - highly educated women's perceptions of gender equality in the workplace. Revija Za Socijalnu Politiku, 24(3), 253-275. doi:10.3935/rsp.v24i3.1432

Wilding, F., & Cyberfeminist International. (1998). Where is feminism in cyberfeminism? (p. 1). na.

Willison, R. & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. MIS Quarterly, 37(1), 1.

https://www.youtube.com/watch?v=IUvnmG3ji-s