Employees' Non-Malicious, Counterproductive Computer Security Behaviors (CCSB) in Nigeria and Canada: An Empirical and Comparative Analysis

Princely Ifinedo
Department of Financial and Information Management,
Cape Breton University,
Sydney, Nova Scotia, Canada
princely_ifinedo@cbu.ca;pifinedo@gmail.com

Boluwaji Ade Akinnuwesi
Department of Computer Science,
Lagos State University,
Ojo, Lagos State, Nigeria
akinboluade@yahoo.com

***Abstract*—Employees indulgence in counterproductive computer security behaviors (CCSB) is a growing phenomenon worldwide. Essentially, CCSB are ill-prescribed computer use practices and general information security behaviors that go against the legitimate interests of an organization. While research on such issues is beginning to emerge in the developed West, information and perspectives from developing countries such as Nigeria is rare in the extant literature. This current study was designed to fill the gap in the literature by providing insights about employees' non-malicious, CCSB in Nigeria and Canada. Data for the study was collected from a field survey and secondary data sources. Relevant data analyses were performed. The results showed that employees' indulgence in CCSB differ by locations or contexts, and importantly socio-economic factors (i.e. national wealth (GDP), transparency, and literacy rates) and the cultural dimensions of individualism versus collectivism (IDV) and uncertainty avoidance (UAI) considered in this study were found to have significant bearings on participants' desire to indulge in CCSB at work. The implications of our findings to both research and practice were succinctly discussed.**

Keywords—counterproductive computer security behaviors; end security behaviors; non-malicious; regression, employees; IS security management

I. INTRODUCTION

In this current information age, organizations around the world have relied (and continue to rely) on information and various computer networks and information systems (IS) that hold valuable organizational data assets and resources [1,2]. In general, computer systems and information technologies (IT) enable organizations to effectively store, process, and utilize information for their operations. Clearly, the use of such technologies poses a serious problem when comprised or breached. Indeed, a variety of setbacks such as financial loss, bad publicity, loss of credibility, legal, and regulatory problems may arise when security breaches occur [4-5].

Threats to an organization's IT resources and data assets can come from within or outside its boundary [6]. Naturally, organizations tend to deploy resources against threats from outside; however, recent industry reports and academic studies continue to show that a substantial proportion of information security threats actually originate from inside the organization [2-7,8]. According to [5], "58% information security incidents attributed to insider threat."

In fact, an organization's employees have been considered the weakest link with regard to ensuring IS security and safety [2,9]. The human agent (i.e., employees), either intentionally or unintentionally engages in ill-prescribed behaviors and practices that can endanger organizational IS resources [8,9]. One example of ill-prescribed behaviors is counterproductive computer security behaviors (CCSB), which refers to employees' computer use practices and general information security behaviors that go against the legitimate interests of an organization. Examples of CCSB considered in this study include visiting non-related websites at work, not updating work-related passwords regularly, and so forth.

The need exists for research to be done in area of CCSB and related insider threats [7,9]. It is worth noting that research in the area is beginning to emerge [6]; however, the majority of studies in the area of end user security behaviors have been conducted in the developed West [6]. Information from the developing parts of the world is rare in the extant literature. Past research have noted that it may not be rewarding for IS/IT issues in technologically advanced societies to be conflated with those in emerging and developing parts of the world. This is because diffusion of technological innovations, acceptance of IS security and privacy practices, indulgence in antisocial computer practices, and so forth have been known to differ by regional locations or contexts [10-12]. Some of the differences have been attributable to socio-economic and cultural underpinnings of societies [13-15].

We argue that for issues related to end user security, in general and CCSB, in particular to be fully understood, researchers must attempt to investigate issues across contexts. Comparative analyses can be made to enlighten insight and inform theory development. Moreover, managers and practitioners in differing contexts can benefit from useful information relevant to their contexts.

This current study is designed to make a contribution in these regards. We decided to choose Nigeria and Canada as research settings for illustration purposes and for the fact that

978-1-4799-4998-4/14/$31.00 ©2014 IEEE

we are familiar with both countries. Additionally, Nigeria is recognized as one the better performers in Africa with respect to IS diffusion issues [16] and Canada is among the top countries in the developed World with regard to IS security and privacy issues [17].

Specifically, the research questions we pose are as follow: **Q1**: Do employees in Nigeria (developing country) and Canada (developed country) perceive the threats of CCSB differently? **Q2**: Do socio-economic and cultural factors have significant relationships and impacts on the employees' desire to indulge in CCSB?

II. BACKGROUND INFORMATION

A. Counterproductive Computer Security Behaviors (CCSB)

Scholarly works on individual information system security behaviors have been loosely classified into two main categories: "white hat" (compliant) behaviors and "black hat" (noncompliant) behaviors [18,19]. According to [19, p.1], "Those in the latter category may be conducted by insiders (e.g. employees) or by individuals outside the organization's boundaries, such as hackers, competitors, or national enemies. Security policy violations by insiders may be non-malicious, such as simple accidental oversights or volitional acts conducted without malicious intent."

TABLE I. THE LIST OF CCSB CONSIDERED IN THE STUDY

No.	*Ref.*	*CCSB*
#1	CCSB1	Responding to spam (i.e. unsolicited emails)
#2	CCSB2	Using weak passwords at work
#3	CCSB3	Not updating work-related passwords regularly
#4	CCSB4	Visiting non-related websites at work
#5	CCSB5	Not updating anti-virus and/or anti-spyware software at work
#6	CCSB6	Not logging out of secure systems after use
#7	CCSB7	Not always treating sensitive data carefully
#8	CCSB8	Allowing one's family (i.e. children) to play with work laptop
#9	CCSB9	Downloading unauthorized software (i.e. freeware) onto work computer
#10	CCSB10	Pasting or sticking computer passwords on office desks
#11	CCSB11	Disclosing work-related passwords to others
#12	CCSB12	Leaving your work laptop unattended

In developing the CCSB considered in this study, we consulted prior literature dealing with such issues [6,8,9,18-20]. In particular, the classification presented in [9] was considered pertinent to this study. Their taxonomy included "high-end" and "malicious" end user security behaviors, e.g. an employee who breaks into an employer's protected IT to steal a trade secret or an "employee [who] configures a wireless gateway that inadvertently allows wireless access to the company's network by people in passing cars", and so forth. Their "low-end" and "non-malicious" end user security behaviors included choosing a bad password and responding to spam email. From [19], examples of non-malicious CCSB included "failing to log off when leaving PC"; In the same vein, Vance et al.'s [8] CCSB include "allowing children to play with laptop" and "sharing passwords". As indicated above and for illustration purposes, this study will focus on "low-end" and "non-malicious" issues; other researchers considered such issues to be relevant in end user security behavior literature [21].

After searching the relevant literature and engaging in a series of informal discussions with practitioners and IS professors, we drew up a list of CCSB, which was pared down to 12 items for illustration purposes (Table I). The items clearly depict internal (insider), "low-end" and "non-malicious" end user security behaviors [8,9,19,20]. In line with our description of CCSB, these acts can lead to disastrous outcomes for an organization's information resources if allowed to occur. For example, employees who share work-related passwords with others, respond to spam emails (laden with Trojan spyware), and leave their work laptops unattended are inadvertently providing means for outsiders to gain access to their organizations' IS resources.

B. Socio-economic and cultural factors

The socio-economic and cultural factors used in this study are discussed next. For illustration purposes, the socio-economic factors considered herein are national wealth (GDP), transparency levels (COPT) and country literacy rates (EDUC). Previous IS security-related studies that considered such factors found them to the pertinent to the discourse [12-16].

National transparency levels refer to the extent to which honesty and fairness prevails in a country [22]. Transparency levels have been reported to be critically important for security- and privacy-related issues [15].Transparency International's [22] website offered data on corruption indices for each country. The scores ranged from "100" (highly uncorrupt) to "0" (highly corrupt).

For the economic variable, we used gross domestic product (GDP) per capita, which refers to a country's gross domestic product divided by its population; it is generally considered an indicator of a country's standard of living or wealth and often used as a differentiator in prior research [10,11,14]. Literacy rates refer to the percentage of people in a country that are literate, that is, able to read and write. This factor has been found to differentiate diffusions technological innovations among countries around the world [10].

Only two cultural factors (i.e., individualism versus collectivism (IDV) and uncertainty avoidance (UAI) from Hofstede's [23,24] cross-cultural typology was used for illustration purposes and for the fact these factors were considered more relevant for IS security and privacy issues [25]. That said, culture is the collective programming of the mind, which distinguishes the members of one group from another [23]; it represents the fabric of meaning through which a society interprets the events around it. National culture tends not only to be ingrained it also influences individuals and group behavior with regard to how they interpret and implement practices within their contexts [26].

Individualism versus collectivism (IDV) refers to extent to which members of a society reinforce individual or collective achievement and interpersonal relationships [23]. Uncertainty avoidance (UAI) refers to extent to which members of a society feel uncomfortable with uncertainty and ambiguity; it

describes tolerance toward risk taking behaviors [23]. Table II shows the socio-economic and cultural indicators for Nigeria and Canada alongside their sources.

TABLE II. SOCIAL-ECONOMIC AND CULTURAL INDICATORS

Indicator	*Nigeria*	*Canada*	*Source*
GDP per capita (2013 estimate)	US$2,800	US$43,100	[27]
Literacy rates (2013 estimate)	61.3%	99%	[27]
National transparency levels (2013)	25	81	[22]
Individualism versus collectivism	30	80	[24]
Uncertainty avoidance	55	48	[24]

III. RESEARCH HYPOTHESES

Individuals from differing localities view issues including those related to information security issues in ways preconditioned by their environments [12,16]. For instance, those with adequate access to technologies or with the opportunity of working in environment supportive of innovative practices and ideas may develop favorable perceptions of such issues as opposed those lacking such resources [16]. Previous studies, insights, and observations suggest that people from differing parts of the world tend to evaluate and adopt technological innovations including IS security and privacy concerns and computer-related antisocial behaviors differently [10-12,15]. Consistent with the foregoing insight, we expect that employees in Nigeria (developing country) and Canada (developed country) would perceive the threats of CCSB differently. Hence, we predict:

H1: There will differences in the perceptions of CCSB among workers base in Nigeria and Canada.

Empirical evidence exists to suggest that innovations diffuse more readily in more affluent societies than in relatively poorer ones [10,11]. This is because poorer societies are still struggling to overcome basic necessities of life, which advanced countries might have overcome [27]. For the same reason, the general awareness of information security and related concerns is high in richer parts of the world [12,13-15] where the general population is known to possess higher literacy levels. Similarly, individuals from societies rife with corruption (i.e. less transparency) may have little or no need for adherence to organizational security guidelines against engaging in CCSB, as such may curtail their unacceptable behaviors [16].

Regarding cultural factors (i.e., UAI and IDV), CCSB can be destabilizing; as such, it is to be expected that individuals from cultures averse to risks will not cope as well as counterparts from more risk tolerant societies [15]. People from individualistic cultures are driven by personal motivations and choices, whereas individuals from collectivistic countries are governed by group norms and aspirations. However, personal action and initiative are conducive to helping contain CCSB; group views mattered less [15]. In light of the preceding evidence supporting the view that socio-economic and cultural factors have are related to technological innovations including IS security and privacy concerns, we expect that such factors would impact the perceptions of CCSB among participants sampled in our study. Hence, we predict:

H2: Socio-economic and cultural factors would have impacts - negative or positive depending on item - on the perceptions of CCSB threats among workers base in Nigeria and Canada.

IV. RESEARCH DATA AND METHODS

A. Socio-Economic Data Variables

Data for the socio-economic variables were obtained from internationally recognized bodies such as the World Bank [27] and Transparency International [22]. These bodies produce cross-country data on a variety of indicators annually. Their data are considered suitable for this study as they have easily accessible indicators of relevance to this present study; more importantly, their data collection efforts allow for cross-national comparison given the fact that they were collected in the same time frame and used comparable methods.

It is worth noting that other researchers comparing issues at the national level have used data from such sources in previous studies [10-16]. For the cultural variables, we used indicators from [23,24], which several prior studies [10-16] have used for similar studies. The socio-economic and cultural used in this study are shown in Table II.

B. Field Study

It is important to stress that this current study is a part of a larger research on the assessment of CCSB across national contexts. We used a field survey to gather relevant information from all contexts including the two countries considered in this study. The survey was administered through a research company, CINT and their affiliate, Fluidsurvey.com. Canadian and Nigerian business professionals from diverse industries with knowledge of CCSB were contacted. The research company gave their panel members points-based incentives redeemable for prizes. The criteria for including participants in the survey are: a) knowledge of CCSB, and b) employment in an organization.

The company's web server reported that 2,209 Canadian and 1300 Nigerian respondents were invited; 1145 participants in Canada and 728 in Nigeria opted to participate in the survey by accepting the consent agreement. The survey was designed such that respondents who indicated indulging in less than 5 CCSB in the last 6 months were prevented from continuing to the next step. In total, 564 Canadian panels were dropped at this stage. Of the remaining 581 responses for the Canadian sub-sample, only 218 were used for data analysis. For the Nigerian sub-sample, 451 panels were dropped, and of the 277 responses, only 81 were considered useable.

Broadly, responses that included monotone or patterned responses, many missing answers, and generally, badly completed surveys, were removed. Overall, the data was checked for violations of assumptions i.e. normality and linearity; the results indicated that these assumptions were met.

In order to present fair information from the collected data, we decided to randomly select 81 responses from the

Canadian sub-sample to match the Nigerian one. Thus, 162 responses were used for this study data analysis.

As per the aspect pertaining to this study, participants were asked to indicate how often they have indulged in the CCSB listed [the 12 items]". Their responses were assessed on a 7-point Likert scale ranging from "Almost never" (1) to "Almost always" (7). The entry for the mean for each CCSB was tabulated and ranked (Tables III).

TABLE III. MEAN SCORE AND RANKING OF CCSB

CCSB	*Canadian*		*Nigerian*	
	Mean (SD)	***Rank***	***Mean (SD)***	***Rank***
Responding to spam (i.e. unsolicited emails)	2.2 (1.7)	11	2.7 (1.7)	9
Using weak passwords at work	4.3 (1.5)	2	3.2 (1.7)	6
Not updating work-related passwords regularly	4.0 (1.7)	5	3.3 (1.9)	5
Visiting non-related websites at work	5.1 (1.5)	1	4.3 (1.7)	1
Not updating anti-virus and/or anti-spyware software at work	3.6 (1.9)	6	3.6 (2.1)	3
Not logging out of secure systems after use	4.2 (2.0)	3	3.8 (2.1)	2
Not always treating sensitive data carefully	2.9 (1.8)	7	2.3 (1.7)	10
Allowing one's family (i.e. children) to play with work laptop	1.9 (1.8)	12	2.8 (2.1)	7[a]
Downloading unauthorized software (i.e. freeware) onto work computer	2.8 (2.0)	8	3.4 (1.9)	4
Pasting or sticking computer passwords on office desks	2.7 (2.1)	9	1.9 (1.6)	12
Disclosing work-related passwords to others	2.5 (1.7)	10	2.0 (1.7)	11
Leaving your work laptop unattended	4.1 (1.9)	4	2.8	7[a]

[a] *A tie in the mean score*

[b] *SD = standard deviation*

V. DATA ANALYSIS AND RESULTS

IBM SPSS 21.0 was used for data analysis. Hypothesis 1 was designed to provide an answer to Q1. In this regard, we used the Mann–Whitney–Wilcoxon (MWW) test, which is a non-parametric statistical test that detects differences in two populations. The results of the test are presented in Table IV.

Hypothesis 2 was designed to provide an answer to Q2. In this aspect, we used correlation analysis and regression analysis. Correlation provides an indication that two variables have some association: negative or positive. Person's correlation analysis was used to assess the strength of the relationships between the study's variables. A correlation coefficient between 0.1 and 0.4 shows a weak association; 0.5 and above show a fairly strong relationship. The correlation matrix of all the study variables is presented in Table V. Several interesting results can be seen from the data. However, correlation between two variables does not indicate that one variable causes the other [28]. To gain better insight on the results we used regression analysis.

Regression analysis is a statistical process for estimating the relationships among variables. The regression model to be estimated in our study is presented in equation 1.

$$Y = \alpha + \beta (X) + e \quad (1)$$

Where α is the unknown intercept, β is the parameter to be estimated, X is the socio-economic and cultural variable in the model, e is the error term of the standard assumption, and Y is each of the 12 CCSB considered in the study.

It is not advisable to perform the regression analysis with all the variables entered at once in the model given the small sample size and the limited number of countries in our study. Instead, we decided to conduct a series of separate regressions with each socio-economic and cultural factor used as the dependent variable.

That said, to enhance the results obtained with respect to Q2, it is recommended that assumptions in the regression analyses are tested [28]. One assumption pertains to multicollinearity, which if existed, could be problematic to data analysis. Multicollinearity exists when two or more predictor variables in a multiple regression model are highly correlated, i.e. values greater 0.7. Table V shows that the results were less than 0.7, in most cases, to indicate that multicollinearity was not a problem in our data.

TABLE IV. MEAN SCORE AND RANKING OF CCSB

Mann–Whitney–Wilcoxon Test Statistics												
	CCSB1	CCSB2	CCSB3	CCSB4	CCSB5	CCSB6	CCSB7	CCSB8	CCSB9	CCSB10	CCSB11	CCSB12
Mann-Whitney U	2582	2159	2478.5	2257.5	3187.5	2832	2683	2418	2808.5	2671.5	2647.5	1951
Wilcoxon W	5903	5480	5799.5	5578.5	6508.5	6153	6004	5739	6129.5	5992.5	5968.5	5272
Z	-2.408	-3.867	-2.728	-3.526	-0.315	-1.525	-2.035	-2.981	-1.602	-2.134	-2.193	-4.507
Sig. (2-tailed)	**0.016**	**0.000**	**0.006**	**0.000**	0.753	0.127	**0.042**	**0.003**	0.109	**0.033**	**0.028**	**0.000**

TABLE V. CORRELATION MATRIX (CONTD.)

	CCSB1	CCSB2	CCSB3	CCSB4	CCSB5	CCSB6	CCSB7	CCSB8	CCSB9	CCSB10	CCSB11	CCSB12
COPT	-.157*	.309**	.209**	.266**	.018	.119	.159*	-.221**	-.123	.204**	.153	.360**
	.046	.000	.008	.001	.817	.130	.043	.005	.118	.009	.051	.000
GDP	-.157*	.309**	.209**	.266**	.018	.119	.159*	-.221**	-.123	.204**	.153	.360**

	.046	.000	.008	.001	.817	.130	.043	.005	.118	.009	.051	.000
IDV	-.157*	.309**	.209**	.266**	.018	.119	.159*	-.221**	-.123	.204**	.153	.360**
	.046	.000	.008	.001	.817	.130	.043	.005	.118	.009	.051	.000
UAI	.157*	-.309**	-.209**	-.266**	-.018	-.119	-.159*	.221**	.123	-.204**	-.153	-.360**
	.046	.000	.008	.001	.817	.130	.043	.005	.118	.009	.051	.000
	162	162	162	162	162	162	162	162	162	162	162	162
EDUC	-.157*	.309**	.209**	.266**	.018	.119	.159*	-.221**	-.123	.204**	.153	.360**
	.046	.000	.008	.001	.817	.130	.043	.005	.118	.009	.051	.000
CCSB1	1	.195*	.094	.055	.280**	.244**	.246**	.208**	.203**	.196*	.191*	.153
		.013	.235	.486	.000	.002	.002	.008	.010	.012	.015	.053
CCSB2	.195*	1	.029	.211**	-.033	.209**	.259**	.030	.047	.362**	.311**	.333**
	.013		.710	.007	.675	.008	.001	.703	.550	.000	.000	.000
CCSB3	.094	.029	1	.018	.199*	.242**	.176*	-.090	-.009	.080	.050	.070
	.235	.710		.819	.011	.002	.025	.254	.913	.310	.528	.378
CCSB4	.055	.211**	.018	1	.012	.315**	.046	-.050	.242**	-.020	.064	.361**
	.486	.007	.819		.882	.000	.558	.524	.002	.798	.417	.000
	162	162	162	162	162	162	162	162	162	162	162	162
CCSB5	.280**	-.033	.199*	.012	1	.075	.225**	.136	.154*	-.021	.009	-.074
	.000	.675	.011	.882		.344	.004	.085	.050	.792	.907	.352
CCSB6	.244**	.209**	.242**	.315**	.075	1	.239**	.063	.165*	.133	.153	.398**
	.002	.008	.002	.000	.344		.002	.428	.036	.092	.051	.000
CCSB7	.246**	.259**	.176*	.046	.225**	.239**	1	.231**	.385**	.270**	.414**	.357**
	.002	.001	.025	.558	.004	.002		.003	.000	.001	.000	.000
CCSB8	.208**	.030	-.090	-.050	.136	.063	.231**	1	.357**	.116	.194*	.184*
	.008	.703	.254	.524	.085	.428	.003		.000	.143	.014	.019
CCSB9	.203**	.047	-.009	.242**	.154*	.165*	.385**	.357**	1	.124	.259**	.198*
	.010	.550	.913	.002	.050	.036	.000	.000		.116	.001	.012
	162	162	162	162	162	162	162	162	162	162	162	162
CCSB10	.196*	.362**	.080	-.020	-.021	.133	.270**	.116	.124	1	.600**	.225**
	.012	.000	.310	.798	.792	.092	.001	.143	.116		.000	.004
CCSB11	.191*	.311**	.050	.064	.009	.153	.414**	.194*	.259**	.600**	1	.350**
	.015	.000	.528	.417	.907	.051	.000	.014	.001	.000		.000
CCSB12	.153	.333**	.070	.361**	-.074	.398**	.357**	.184*	.198*	.225**	.350**	1
	.053	.000	.378	.000	.352	.000	.000	.019	.012	.004	.000	

Seeing no problems with the data, we performed a series of regression analyses. A summary of some the results are presented in Table VI (we omitted the others due to space limitations). All the five socio-economic and cultural variables were found to have significant impacts on the majority of the study's CCSB with the exception of only four CCSB (#CCSB5, #CCSB6, #CCSB9, and #CCSB11). In other words, none of the socio-economic and cultural variables had significant results for the four items.

TABLE VI. REGRESSION ANALYSES' RESULTS (CONTD.)

Independent variables	***Dependent CCSB***	***Results***		
		R^2	β	***Sig.***
EDUC	CCSB1	0.03	-0.16	0.046

EDUC	CCSB2	0.10	0.31	0.00
UAI	CCSB1	0.03	0.16	0.046
UAI	CCSB2	0.10	-0.31	0.00
COPT	CCSB1	0.02	-0.16	0.046
COPT	CCSB12	0.13	0.36	0.00
GDP	CCSB8	0.05	-0.22	0.05
GDP	CCSB8	0.05	0.21	0.08
IDV	CCSB4	0.07	0.27	0.01
IDV	CCSB7	0.03	0.16	0.043

VI. DISCUSSIONS

The purpose of this study is to compare the employees' perceptions of threats of CCSB. Two countries (i.e., Nigeria and Canada) with differing socio-economic and cultural factors were chosen mainly for illustration purposes. Specifically, we wanted to know whether employees from both countries assess the threats of CCSB differently given the suggestions and espoused information from prior research and insights.

In this aspect, our data analysis provided partial support for hypothesis 1. Participants' perceptions of 9 out of 12 CCSB differed significantly. There were no differences in perceptions of threats related to CCSB5, CCSB6, and CCSB9. There were also remarkable results as well. For example, participants from both countries equally agreed that they are more likely to visit non-related websites at work (CCSB1). There were similarities in how participants from both countries responded to CCSB3 and CCSB11.

In all, participants from Canada indicated that they are more likely to indulge in CCSB than their Nigerian counterparts in almost all the CCSB considered in this study with the exception of CCSB1, CCSB8, and CCSB9, which Nigeria participants had higher mean scores than their Canadian counterparts. This study was not designed to provide an answer as to *why* such was the case. However, we contend that socio-economic and cultural factors might help shed some useful light in such discourse.

Our second inquiry (Q2) aimed to enlighten on whether socio-economic and cultural factors have significant relationships and impacts on the employees' desire to indulge in CCSB. The results of our regression analysis also provide partial support for H2. Namely, the socio-economic factors of national wealth, transparency, literacy levels, and the cultural dimensions of UAI and IDV were found to have significant impacts on employees' desire to engage in almost all the CCSB considered herein with the exception of (#CCSB5, #CCSB6, #CCSB9, and #CCSB11).

A. Contribution to Research

From a theoretical perspective, this study has enriched the literature with its endeavor that attempts to compare employees' perceptions of CCSB at work from two differing national or geographical contexts. Diversification and comparisons of findings in research augurs well for theory development and knowledge accumulation in the area. The insight regarding workers' perceptions of CCSB adds to the body of work focusing on end user information security behavior [6]. Our results also lend support to observations in the extant literature that signify the pertinence of national cultural factors and socio-economic influences on IT/IS security management in organizations [10-16]. This effort may spur further research in the area.

B. Practical Implications

The benefits to practitioners are as follows: The attention of practitioners is drawn to the importance of contextual influences (socio-economic and cultural factors). Such information may offer insights that strengthen the management of workers' desire to indulge in CCSB across contexts. The importance of information provided herein is that workers from across differing contexts may behave differently regarding their urge to engage in CCSB. For example, workers from Canada are more likely to leave their work laptop unattended (mean = 4.0); the same is not true for Nigerian workers (mean = 2.8). In developed and richer societies, computers are not considered a luxury good. The same view may not be true in relatively poorer countries where such are seen as elitist tools. Further to this, workers from Canada indicated that they are more like to use weak passwords at work (mean = 4.3); their Nigerian counterparts are less inclined to do so (mean = 3.2). We have to stress that the foregoing information need to be interpreted in the context of our research.

Notwithstanding, the management of multi-national organizations can benefit from the information provided in this study as they promote organizational IS security policies and acceptable practices and procedures that take into account regional differences (and similarities) . For example, they may have a need to provide more focused awareness campaigns, training or education in regions where certain CCSB are likely to occur. It is important to emphasize the fact that it would be erroneous to accept that all workers/employees across differing locations or regions hold exactly the same view of CCSB or behave in a similar way toward such and that environmental factors such as national culture and socio-economic conditions do not matter. Our study showed that such have critical roles in the discourse. In the same vein, the assessments and evaluations of IS development project risks and threats across contexts also benefits from this effort [29].

C. Limitaions of the Study and Future Research Avenues

The study clearly has its limitations. For example, in some aspects, it used data obtained from secondary sources. As a result, it might have inherited all limitations from those sources. With respect to the field research data; the following limitations are highlighted. First, the data came from a cross-sectional field survey; longitudinal data may facilitate more insight. Second, participants might have provided socially desirable responses to some of the questions to negatively impact the results. Third, the data came from two countries; a larger sample of sample might offer more useful insights. Fourth, the sample size is small; a large pool of respondents is valued.

Future study should endeavor to overcome the shortcomings in this study. Attention should be paid to other end user security behaviors, such as high-end malicious CCSB, in future studies. Studies using observations and employees' actual engagement in CCSB and related behaviors could be more informative.

VII. CONCLUSION

This study has shed some light on the issue of CCSB with information garnered from two contrasting parts of the world: developed and developing countries. The study's results provide partial support that suggests that employees' desire to engage in CCSB differ by locations or contexts. This current study also signified the critical importance of socio-economic factors and the cultural dimensions of UAI and IDV to workers' desire to indulge in CCSB at work. It is hoped that this study's findings will spur on further research and inquiries in the area. Practitioners from across differing contexts could use the information provided in this study to better manage workers' urge to engage in CCSB.

VIII. ACKNOWLEDGMENT

Funding for this study was received from Social Sciences and Humanities Research Council of Canada (430-2013-000879).

REFERENCES

[1] T. H. Davenport, and J. E. Short, "The new industrial engineering: Information technology and business process redesign," MIT Sloan Mgt. Rev. vol. 31, iss. 4, pp. 11-27, 1990.

[2] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," Inform. & Mgt. vol. 51, iss. 1, pp. 69-79, 2014.

[3] D. H. Andrews, J. Freeman, T. S. Andre, J. Feeney, A. Carlin, C. M. Fidopiastis, and P. Fitzgerald, "Training organizational supervisors to detect and prevent cyber insider threats: two approaches," EAI Endorsed Trans. on Sec. and Safety. vol. 6, iss. (1-6), pp. 1-7, 2013.

[4] Q. Hu, Z. Xu, T. Dinev, and H. Ling, "Does deterrence work in reducing information security policy abuse by employees?" CACM. vol.54, iss. 6, pp. 54-60, 2011.

[5] Inform Security Magazine, News. http://www.infosecurity-magazine.com/view/32222/58-information-security-incidents-attributed-to-insider-threat-, 2013.

[6] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," Compt. & Sec. vol. 32, iss. 1, pp. 90-101, 2013.

[7] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," MIS Quarterly. vol. , 34, iss 3, pp. 523-548, 2010.

[8] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from habit and protection motivation theory," Inform. & Mgt. vol. 49, pp. 190-198, 2012.

[9] J. M. Stanton, K. R. Stam, P. Mastrangelo, and J. Jolton, "Analysis of End User Security Behaviors," Compt. & Sec. vol. 24, iss. 2, pp. 124-133, 2005.

[10] D. D. Gregorio, S. K. Kassicieh, and R. D. Neto, "Drivers of e-business activity in developed and emerging markets," IEEE Trans. on Eng. Mgt. vol. 52, iss. 2, pp. 155-166, 2005.

[11] D. Comin, and B. Hobijn, "An exploration of technology diffusion," Amer. Econ. Rev. vol. 100, iss. 5, pp. 2031-2059, 2010.

[12] K. Bagchi, P. Kirs, and R. Cerveny, "Global software piracy: can economic factors alone explain the trend?" CACM. vol. 49, iss. 6, pp. 70-75, 2006.

[13] P. Ifinedo, "Information technology security concerns in global financial services institutions: do socio-economic factors differentiate perceptions?" Internl. J. of Inform. Sec. and Priv. vol. 3, iss. 2, pp. 68-83, 2009.

[14] P. Ifinedo, "An exploratory study of the relationships between selected contextual factors and information security concerns in global financial services institutions," J. of Inform. Sec. and Priv. vol. 7, iss. 1, pp. 25-49, 2011.

[15] P. Ifinedo, "Information technology security management concerns in global financial services institutions: is national culture a differentiator? Inform. Mgt. & Compt. Sec. vol. 17, iss. 5, pp. 372-387, 2009.

[16] P. Ifinedo, "Measuring Africa's e-readiness in the global networked economy: a nine-country data analysis," The Internl. J. of Educ. and Dev. using Inform. and Comm. Tech. vol. 1, iss. 1, pp. 53-71, 2005.

[17] 2012 DTTL Global Financial Services Industry Security Study Breaking Barriers. Retrieved October 3, 2013, http://www.deloitte.com/view/en_GX/global/industries/financial-services/42a6436f82559310VgnVCM2000001b56f00aRCRD.htm#.Ukxb34aTjmc.

[18] M. A. Mahmood, M. Siponen, D. Straub, R. Rao, and T. S. Raghu, "Moving toward black hat research in information systems security: An editorial introduction to the special issue," MIS Quarterly, vol. 34, iss. 3, pp. 431-433, 2010.

[19] M. Warkentin, D. Straub, K. and Malimage, "Featured talk: measuring secure behavior: A research commentary," Annual symposium on information assurance & secure knowledge management, June 5-6, 2012.

[20] K. D. Loch, H. H. Carr, and M. E. Warkentin, "Threats to information systems: today's reality, yesterday's understanding," MIS Quarterly. vol. 16, iss. 2, pp. 173-186, 1992.

[21] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding nonmalicious security violations in the workplace: A composite behavior model," JMIS. vol. 28, iss. 2, pp. 203–236, 2011.

[22] Transparency International. Corruption Perception Index – 2013. Retrieved June 1, 2014, http://www.transparency.org/. 2013.

[23] Hoftstede, G., Culture's Consequences. Thousand Oaks, CA: Sage Publications, 2001.

[24] Hofstede, G., "The Hofstede centre - National culture, countries," http://geert- hofstede.com/. Retrieved July 23, 2014.

[25] P. Ifinedo, "The effects of national culture on the assessment of information security threats and controls in financial services industry," Internl. J. of Electron. Bus. Mgt. vol. 12, iss. 2, pp. 75-89, 2014.

[26] M. Černe, M., Jaklič, and M. Škerlavaj, "Decoupling management and technological innovations: Resolving the individualism–collectivism controversy," J. of Intl. Mgt. vol. 19, iss. 2, pp. 103-117, 2013.

[27] World Bank, "World Economic Indicators," Retrieved June 13, 2014, http://data.worldbank.org/data-catalog/world-development-indicators, 2014.

[28] J. F. Jr., Hair, R. E. Anderson, R. L. Thatham, and W. C Black, Multivariate Data Analysis. Upper Saddle River, NJ: Prentice-Hall International, Inc., 1998.

[29] Uwadia C. O., Ifinedo, P. E., Nwamarah, G. M., Eseyin, E. G., and Sawyerr, A. "Risk factors in the collaborative development of management information systems for Nigerian universities," Inform. Techn. for Dev. vol. 12, iss. 2, pp. 91-111, 2006.