Conceptual Modeling of Social Factors Using Social Control (Nigeria Context)

[1]Gbenga T. Omoniyi, [2]Dr. Shahrudin Awang Nor, [3]Nor Iadah Yusop, [4]Rotimi-Williams Bello
[1,] Awang Had Salleh Graduate School, UUM College of Arts & Sciences, Universiti Utara Malaysia
[2]SETARA, PPPM (PT) & Rating Manager, Strategy Planning Division, Institute of Quality Management, Universiti Utara Malaysia
[3]School of Computing, UUM College of Arts & Sciences, Universiti Utara Malaysia
[4]Department of Mathematical Sciences, University of Africa, Toru-Orua, Bayelsa State, Nigeria
Email: [1]geegartea@yahoo.com, [2]shah@uum.edu.my, [3]noriadah@uum.edu.my, [4]sirbrw@yahoo.com

Abstract: *Social control is a sociological idea which refers to a system that manages individual and group actions, prompting congruity and consistence with the policies of a given society or social gathering. In general, formal social control is communicated through law as statutes, decrees, and instructions against immoral actions; while informal social control depends on traditions, customs, beliefs, standards, ethical quality or other social esteems and usually fulfilled by unofficial regulatory groups or a person. In respect to different principles, social control can be separated into various sorts. In this study, we integrated general deterrence theory (GDT) and social bond theory (SBT) by utilizing two essential types of social control; formal and informal social control to propose a conceptual model.*

Key Words: *Social, Belief, Ethical, Customs, Traditions, Decrees, General deterrence theory (GDT), Social bond theory (SBT)*

1. INTRODUCTION:

There has been different definition of social factors over the years based on respective researcher's field of study, but the common definition is that social factors are experiences and facts that influence an individual's attitudes, personality and lifestyle. Since the main objective of this study is to integrate general deterrent theory (GDT) and social bond theory (SBT) using social control to propose conceptual model for social factors, there is need to foremost explain how these certain factors are considered to be social factors based on previous studies. According to social cognitive theory (SCT) proposed by [1]; the theory offers that three fundamental requirements must be in place before human behaviour can be identified, the requirements are: (1) personal factors (2) behaviour (3) the environment. When discussing the innovation of behavioural change strategies, behavioural theory plays a vital function, and this is why the choice of behavioural theory (BT) is essential. Although, several BT's are known to have limitations, SCT is one of the exempted among the most significant ones, and it has been utilized in steering several behavioural interventions [2].

SCT is a learning hypothesis expressing that individuals acquire certain knowledge by watching and emulating others and by encouraging feedback. It also places that behavioural change is always influenced by three factors namely: (1) personal factors (2) behaviour (internal nature) (3) environmental influences. In other words, behavioural change can be regarded as a complex procedure that is impacted by both internal and external factors [3]. SCT as one of the examples of BT is basically model of the impacts on behaviour and their interconnections, and they are agreeable to several modeling techniques. Vigorous computational modeling methodologies would give a more adaptable and thorough experimentation of SCT, together with other behavioural theories (BTs) that are prone to affirm, modify, or discredit SCT. In addition, computational models can improvably help in determining framework pertinent and momentary interconnections that would now be able to be measured constantly after some time [2]. Since SCT is one of BT's with no limitation and quite valid in analysing behavioural change strategies as well as understanding behavioural intentions, needless to say further that the issue of Internet crime involves humans behavioural analysis in other to understand the concept behind the act and how to protect Internet users from falling victim. For the purpose of this study, knowledge (personal factor) happens to be an essential factor among the three factors required to complete the SCT circle, that makes it as essential as the other two factors, which explains why knowledge is considered as a viable social factor required for this study.

GDT is a well-established theory in the information systems (IS) security field [4] and has been connected with a specific end goal to dissuade Internet abuse. Security Action Cycle is an example of its application [4]. As indicated by the above model, Internet abuse must be assessed at four phases:

(i) Deterrence: The greater part of the potential perpetrators is deterred via techniques like: regulations, policies, awareness programs and decrees.

(ii) Prevention: In the event that deterrence ends up being insufficient, prevention techniques are utilized, for example, physical or procedural controls.

(iii) Detection: The techniques at this level address the acknowledgment of Internet abuse, intending to make such abuse known.

(iv) Remedies: At the point when Internet abuse is identified, its outcomes ought to be dealt with properly; activities against the perpetrators ought to be handled, as indicated by the organization's rules and policy.

SBT is a prominent theory in criminology, which tries to clarify social actions that do not obey the popularly accepted social standards. It depends on the hypothesis that regardless of a man's usual feeling towards committing crime, solid social bonds discourage him/her from perpetrating criminal acts. Under this suspicion, the likelihood of a man being engaged with crime increases when social bonds turn out to be weaker [5]. [6] characterizes four types of social bonds that advance socialization and compliance:

(i) Attachment: This denotes an individual's consideration for his/her social environment. The level of assent or agreement to social standards and the improvement of social awareness rely upon the attachment of a person to other individuals. Most vital social societies comprise family, school and colleagues [5].

(ii) Commitment: The commitment to conventional objectives depends on the thought that individuals who devote time, vitality and exertion in accomplishing societal position, education, property or standing status are more averse to participate in criminal acts that may put their accomplishments at risk [5].

(iii) Involvement: Engaging in socially accepted activities, such as school, family, work or leisure, allows limited time available for an individual to get involved in criminal acts [5].

(iv) Belief: Finally, when there is lack or inadequacy of confidence in social esteems, the likelihood of an individual involving in unconventional acts upsurges [5].

Having considered the theories of both GDT and SBT, the paper objective is to integrate the two theories using social control to propose a conceptual model adapted from [7].

2. LITERATURE REVIEW:

Social control is a sociological idea that was first proposed by [8], which refers to a system that manages individual and group actions, prompting congruity and consistence with the policies of a given society or social gathering [8]. In respect to different principles, social control can be separated into various sorts. In this study we utilized two essential types of social control; formal and informal social control. In general, formal social control is communicated through law as statutes, decrees, and instructions against immoral actions; while informal social control depends on traditions, customs, beliefs, standards, ethical quality or other social esteems and usually fulfilled by unofficial regulatory groups or a person [9], [10], [7]. The social control system has been basically utilized in social deviant behaviours. In general, criminal actions can be averted by formal control that utilizes law and authority government bureau to endorse conformity, or by informal control which utilizes ethics and social organizations to urge individuals to abide by the law. It's difficult to state which of the two controls is more efficient since individuals may have different religion, ethics, morals, principles and be in distinct social condition. Generally, both formal and informal controls are mixed to discourage crime with an accentuation towards formal control systems being pervasive [7].

Because organization can also be referred to as a social group or gathering, [7] proposed that social control systems can be applied to organizations too. Organizations create several laws and regulations to enable workers to be equipped with moral esteems and principles. This is a formal control to limit workers' deviant conduct and these may work in conjunction, as said to other formal controls set up. Formal controls functions as the action taken by the organization when workers violate the rules. There is an additional social control system inside the organization which is informal control; another essential restriction that confine workers' actions. It originates from a workers' self-examination about their associations with others and that from considering external pressures [7]. Enormous amount of studies only examine the technical and formal controls for IS security management; however security administration at informal level has been hardly stressed.

Social systems can be simply characterized as far as basic arrangements of shared expectations for behaviour. At that point, accountability may be thought of as the cement that ties social systems together. Without the ability to call a particular individual to be responsible for their actions, there is no foundation to social order, for common desires, or perhaps, for the support of a social system. Organizational reactions to the necessity for accountability from its followers (or in the case of this study, Internet users) involves the creation of procedures or methods such as performance assessments and monitoring, formal reporting relationships, reward scheme, disciplinary methodology, supervisory administration training, personnel manuals, occupational contracts, etc. [11]. [12] suggested that the key part to managing cyber-physical systems is to develop theory of accountability that includes both control and computing systems. Furthermore, the study emphasized that a robust and unifying accountability theory can be established on the basis of causal information flow study, the theory will bolster outline and examination of mechanisms at different phases

of the accountability administration such as: (1) attack/assault detection (2) duty task (e.g., attack localization) (3) remedial measures (e.g., by means of flexible control) [12]. According to [13], means of managing accountability in the design of (IS) can be divided into three methods namely: (1) interactive accountability approach (2) regulatory accountability approach (3) participatory accountability approach.

The obligation of building up a valuable theoretical framework for investigating accountability begins by taking note of the points of view grew so far by two groups of scholars. The first scholarly perspective mainly include social psychologists and ethno-methodologists, with focus concentration on the accountability of conduct (AC); the other group, involving political researchers with a legal or institutional inclination, have been oriented with the conduct of accountability (CA). Regardless of apathy toward each other's work, the two groups give a shared underpinning to the present work. The AC/CA approaches are very particular at first glance. The AC group looks to the utilization of justification or excuses by people who confront circumstances where mistakes or ostensive disappointment have rendered them accountable to some other individual or group. There is an experiential attempt focused on explaining and/or potentially illustrating a typical human behaviour. When they consider an occasion of accountability in government, it is only a simple one more instance of a non specific activity. While the distinguishing governmental setting has an effect, it is not the main emphasis of concentration; the floor of the council might also be the manufacturing plant floor or the swarmed elevator. What is most essential is the manner by which and why people represent their (usually incorrect) behaviour to others [14].

The CA group, conversely, has a tendency to be more institutional in its concentration and standardize in its intent. Their emphasis has a tendency to be on the structures and process through which accountability is accomplished, and they usually relate to the context (i.e., executive or legislative, private or governmental) as significant. As a subsection of that general group, pupils of administrative system and public administration have participated in discussion over the relative significance of various types of accountability, in many cases giving more regard for the standardization than the experimental attempt. In addition, both methods require mental focus in a valuable conceptualization of accountability. Both points of view independently deduced the investigation of public administrative behaviour separately from the essence of its accountability. The AC approach does feature the part accountability plays for the individual both socially and mentally, however applying it out without due thought for the institutional setting undervalues the importance and distinguishing function performs by the governmental context. The CA point of view, on the other hand, trivializes or distorts the impact of individual psychology and social flow in the structures and process of established accountability systems. The requirement for our conceptualization of accountability, consequently, is a system that incorporates both the nonconformist AC and the institutionalise CA perspectives.

Nonetheless, such a conceptualization must be joined by a hypothetical reorientation that will examine more closely the connection between the two levels of study denoted by those points of view [14]. Lately, there has been incredible enthusiasm for several accountability mechanisms that depend on after-the-fact authentication. The fright of getting "caught" accomplishes security by discouragement, in the disposition of conventional law enforcement and organizational security. Accountability assumes an essential part in the development of trust amid human interaction. In this way, accountability is seen both as an instrument to accomplish realistic security and as a top notch design objective of services in federated distributed systems. While scheming for accountability is astute by and large, methods to instrument systems in assisting accountability have been investigated in a few particular applications: network storage, authenticating ISP quality of service claims, determinate distributed systems, and Internet protocol and policy imposition on shared archives. In relationship with some earlier approach, for instance, access-control, be that as it may, the accountability method to deal with security needs general basis for models and programming [15].

3. METHODOLOGY:

The method used in this paper was adapted from [7]. The two types of social control; the formal and informal social control were used to integrate general deterrence theory (GDT) and social bond theory (SBT) for conceptual modelling of social factors.

3.1 General Deterrence Theory:

General Deterrence Theory (GDT) was first initiated by [16] as shown in Figure 3.1, and it has since been broadly utilized as part of the research of criminal and antisocial behaviour and is a settled theory in the field of criminology. Several adaptation and modifications have been introduced by different scholars [4], [5], [17], [7] over the past years, but the basic concept remains that the GDT relies on the speculation that people settle on sensible choices in view of the expansion of their advantage and the minimization of cost [5]. It concentrates on the 'disincentives' or sanctions against carrying out a criminal act and their efficiency as a restriction. Studies [5], [4] recommend that the efficiency of such deterrents depend on: (1) certainty of sanctions (2) severity of sanction. This theory proposes that when the likelihood of penalty is high and the sanction is extreme, potential perpetrators will be discouraged from involving in criminal acts, particularly when their intentions are feeble. Considering insider abuse as common,

professional crime, it happens in a somewhat considerate environment, by individuals who normally abide by rules and regulations. In this specific circumstance, sanctions are considered to be efficient on the grounds that, however, workers may want to ignore their respective social norms in other to profit, but their intentions are feeble and, consequently, deterrence systems can demonstrate to be efficient [4], [5]. GDT is a well-established theory in the IS security field [4] and has been connected with a specific end goal to dissuade Internet abuse. Security Action Cycle is an example of its application [4]. As indicated by the above model, Internet abuse must be assessed at four phases:

(i) Deterrence: The greater part of the potential perpetrators are deterred via techniques like; regulations, policies, awareness programs and decrees.
(ii) Prevention: In the event that deterrence ends up being insufficient, prevention techniques are utilized, for example, physical or procedural controls.
(iii) Detection: The techniques at this level address the acknowledgment of Internet abuse, intending to make such abuse known.
(iv) Remedies: At the point when Internet abuse is identified, its outcomes ought to be dealt with properly; activities against the perpetrators ought to be handled, as indicated by the organization's rules and policy.

3.2 General Deterrence Theory as Formal Control:

Formal controls are vital in molding people's action. This type of control works through the regularized rules and relating sanctions built up by the organization. Organizations depend on formally founded negative sanctions like expulsion, relegation, and suspension to support congruity with organizational behaviour expectations. The Information System Security Policy (ISSP) should unmistakably characterize unsuitable or illicit actions, thus amplifying the perceived threat of penalty [7]. In respect to recent highlight on GDT, as a criminological theory that standout amongst the most broadly utilized theory in information security field [4], [18], [7]. GDT was initially created to clarify how to keep individuals from taking part in deviant actions. It lays on the suggestion that human conduct is to some degree sensible, and consequently can be impacted by inducement, especially the negative inducement characterized in

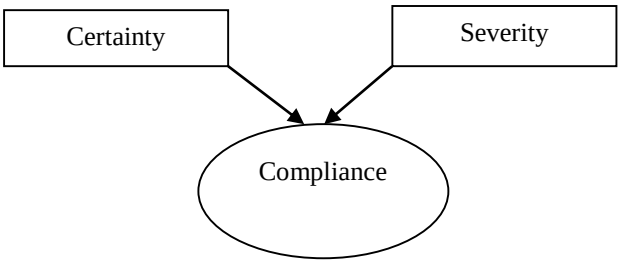

Figure 3.1: General Deterrence Theory (GDT) (Goodhue and Straub, 1991)

formal sanctions [7]. As previously stated, the two focal principles incorporated into the theory are: (1) sanction certainty (2) sanction severity. Certainty implies that an individual trusts that his or her criminal actions will be identified, while severity implies that it will be brutally penalized. The higher the certainty and severity of sanctions for criminal behaviour, the more the people deterred from such behaviour [7].

Sanction severity and sanction certainty were both adversely related to the aim of participating in deviant actions in working environments, for example, cyber loafing, using organizational equipment for personal purpose and IS abuse [18]. Research based on GDT, emphasize sanctions as a critical instrument to deter IS security infringements and consequently enhancing IS security. [19] found that expressing punishments for ISSP infringement builds security conduct. Sanctions may contain penalty techniques, for example, censures, fines, job termination, imprisonment and others. Active and visible endeavors can diminish IS abuse by persuading potential perpetrators that the likelihood of penalty is extremely high. These will demoralize illicit behaviour by expanding its intimidated or perceived costs. For lowering these risks, workers will better abide by the rules and regulation [7].

3.3 Social Bond Theory:

In the process of understanding Internet user's compliance to policy that will deter them from Internet crime, the social bond theory (SBT) was applied. The SBT has drawn the interest of specialists as of late. [6] proposed the SBT and contended that men are inherently inclined to aberrance. The SBT depicts how people, who have more grounded social ties, draw in less in deviant actions. This is a remarkable point in this theory that urges this study to utilize it. Aberrance happens when the social bond is powerless or broken. Attachment, Involvement, Commitment and Belief are the four principle components in this theory. These parts are different, yet interrelated [20]. The SBT is a prominent theory in criminology, which tries to clarify social actions that do not obey the popularly accepted social standards. It

depends on the hypothesis that regardless of a man's usual feeling towards committing crime, solid social bonds discourage him/her from perpetrating criminal acts. Under this suspicion, the likelihood of a man being engaged with crime increases when social bonds turn out to be weaker [5]. [6] characterizes four types of social bonds that advance socialization and compliance:

(i) Attachment: This denotes an individual's consideration for his/her social environment. The level of assent or agreement to social standards and the improvement of social awareness rely upon the attachment of a person to other individuals. Most vital social societies comprise family, school and colleagues [5].

(ii) Commitment: The commitment to conventional objectives depends on the thought that individuals who devote time, vitality and exertion in accomplishing societal position, education, property or standing status are more averse to participate in criminal acts that may put their accomplishments at risk [5].

(iii) Involvement: Engaging in socially accepted activities, such as school, family, work or leisure, allows limited time available for an individual to get involved in criminal acts [5].

(iv) Belief: Finally, when there is lack or inadequacy of confidence in social esteems, the likelihood of an individual involving in unconventional acts upsurges [5].

[21] investigate the efficiency of the SBT theory as to computer abuse in organizations. Their discoveries uncover the critical part that social bonds play in dissuading potential criminal behaviours. [21], has additionally investigated the use of the SBT with respect to IS security, and concluded that the constructive opinion of crime can lead an individual to perpetrating criminal activities in spite of the high peril of penalty. [22], demonstrates that workers will probably take part in criminal acts when their attachment to the organisation is feeble. They further tests the efficiency of integrated models of GDT and SBT in dealing with the IS insider risk. This study investigates how factors from the GDT like security policy can influence Internet crime in Nigeria and whether if integrated with social factors like attitude and knowledge coupled with the four factors of the SBT (attachment, commitment, involvement and belief) as shown in Figure 3.2 can as well influence Internet crime in Nigeria.

3.4 Social Bond Theory as Informal Control:

With a specific end goal to better understand how social factors influence Internet crime in Nigeria, this study utilizes SBT as part of the foundation of our theoretical model for informal control. SBT has been utilized by numerous criminal behavioural studies, yet it has been once in a while utilized as a part of the field of IS security. SBT (also known as social control theory, SCT) was proposed by [6] as earlier stated in this study. [6] argues that people are intrinsically prone to aberrance. It is just the restriction invoked by regulating institutions that represses people from involving in such criminal acts. [6] suggested that the four components of the SBT are different, however interrelated. SBT envisages that the more intense an individual is fused to conformist society, the lower the tendency that he/she will diverge from those socially accepted norms and get involved in criminal conduct.

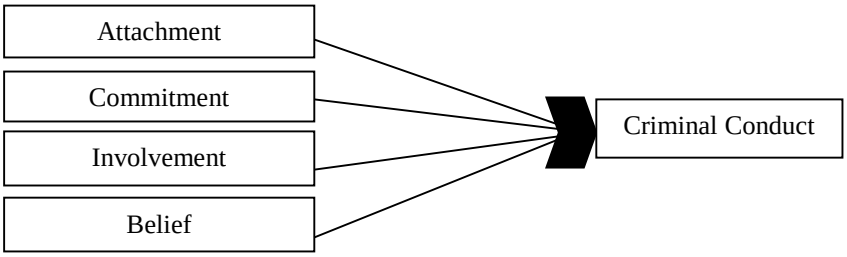

Figure 3.2: Social Bond Theory (SBT)

[22] demonstrated that social bond factors importantly influence insiders' computer abuse. As indicated by [6] postulation, individuals who have more concrete ties with the social community will probably adhere to the community rules. In the organization information security setting, the impacts of such bonds still works, and this impacts workers' ISSP infringement aim. The foremost element of bond, which is attachment, depicts the fondness and regard that a person has with their associates [6]. [6] mentioned parents, teachers, schools and friends as probable associates. In the context of Nigeria as a community, the associates may likely to be, spouse, colleagues, teachers, co-workers, friends, the country (Nigeria). As indicated by social bond theory, people with concrete attachments have fewer tendencies to get involved in criminal behaviour [7]. The greater extent at which a person is bonded to their organization, the less likely they tend to diverge from such organization's policies [20]. Past studies have likewise utilized the SBT to clarify the criminal behaviour of youths.

Their attachment to traditional associate, their commitment to the activities of ordinary objectives, their involvement in standard exercises, and their belief in the legitimacy of normal value system influence their criminal behaviour [20]. In this circumstance, they either disregard, or neglect to do what the law or obligation requires [20]. The extent of SBT applications was stretched out to adult delinquency and authoritative deviances. [7] and [23] have depicted

how the consistence of workers behaviour with information security strategies and policies bring down the danger of information security violation in organizations. In accordance with these past studies, we are utilizing the social bond factors in this study. Attachment to Nigeria as a community, commitment to government's policies and plans, involvement in information security, and the individual belief that obeying the government's information security policies and techniques can influence Internet crime in Nigeria.

3.5 Conceptual Model:

This section displays the conceptual structure that depicts the social variables that are understudied. The conceptual model shows the connections between the social factors that are considered as the determinants that influence Internet crime in Nigeria (Figure 3.2). The connections of the variables were hypothesized**.**

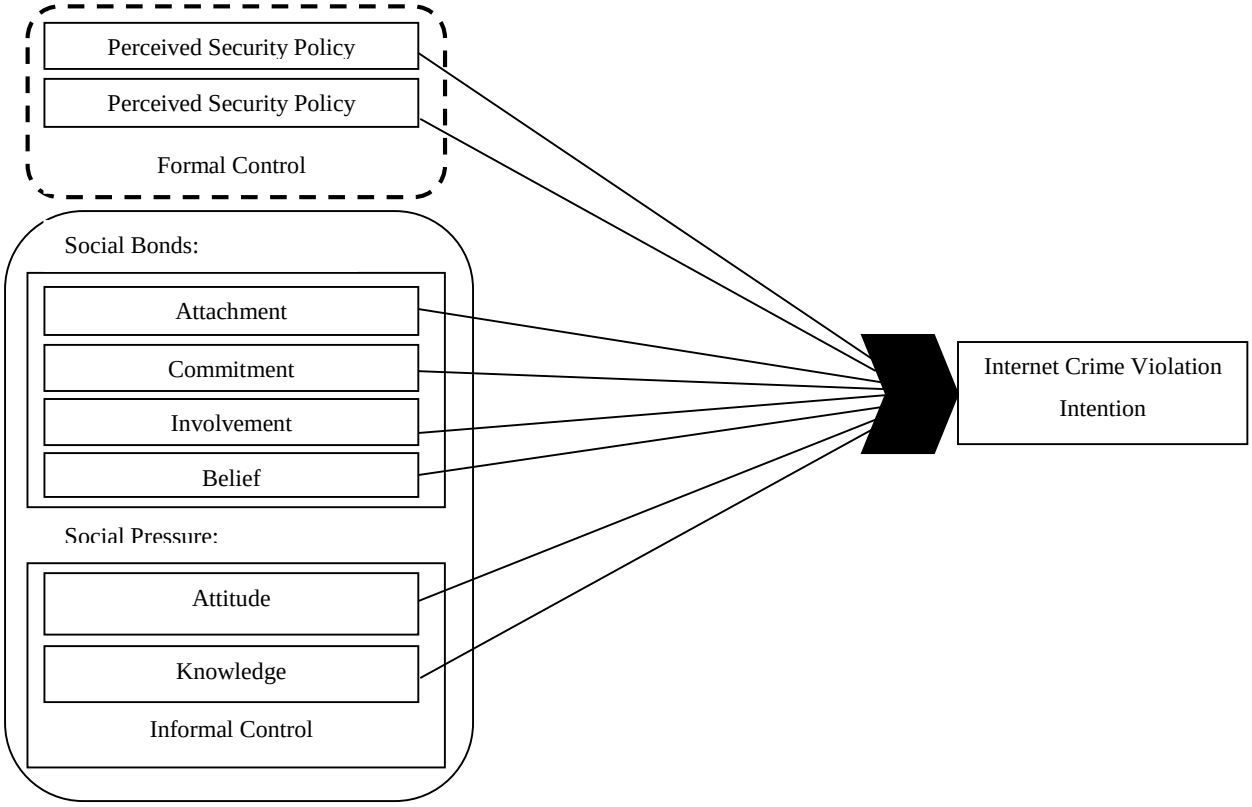

Figure 3.3: Conceptual Model (Adapted from Cheng et al., 2013)

Deducing from the theoretical arguments and reviews of past relevant studies, this study has found that social variables extensively play a vital role in tackling Internet criminals and their offensive activities. This study integrated two theories that are well established in social control perspective to understand how social factors influence Internet crime in Nigeria and to also propose a model showing the relationship to support the study. The adopted theories are SBT and GDT coupled with informal control social factors such as attitude and knowledge. The social variables that were theoretically adopted from the GDT are certainty and severity in relative to security policy as a formal control social factor. While on the other hand, the whole four factors of the SBT that were adopted are attachment, commitment, involvement and belief. The impacts of these variables on Internet crime in Nigeria were examined. Integrating GDT and SBT to assessing human compliance intention is not a common undertaking, but few scholars [7], [22], [21] have done this in past studies with positive outcomes, which is why this study adopted such procedure in examining Internet crime in Nigeria. In respect to [7] studies, that stated that, in other to effectively evaluate human compliance or behavioural intention, two social control methods need to be applied, and they are (1) formal and (2) informal control system. The formal control is basically stressed to be a control system that involved regulatory institution, organization, or perhaps the government for the purpose of this study.

And in other to implement such control system to influence people's behaviour, it need to be imposed in form of sanctions or penalties against any criminal acts, these sanctions are to clearly specify the unacceptable behaviours from the people which will then influence how they perceive threat of the penalty. Based on the fact that the GDT is popularly known to be an efficient theory in information security sector, and for the fact that [7] was able to apply it as a formal control system to effectively support their studies in developing a model which this study adopted. The GDT in this study regarded security policy as the sanctions and based on GDT two popular factors that evaluate how people comply with any rules; they are: (1) severity (2) certainty. The effect of socially acceptable moral standards on humans'

behaviour is a reflection of informal control system [7]. The study further explained that the relationship, ties or bond that an individual establish with their organization, environment or community coupled with pressure from other external factors always have influence on such individual's actions. [7] used the SBT as an informal control system for their model and integrated it with the GDT, which is why this study adopted similar method to examine the influence of these social factors on Internet crime in Nigeria.

Attachment happens to be the first social factor in the SBT and for this study, it examined if Internet users have affection and respect for Nigeria as a community enough before deciding on the nature of activities to engage in. While commitment is to depict if such Internet users have the zeal or focused on attaining career advancement and constructive information acquisition on the Internet in the community over getting involved in Internet crime. Involvement on the other hand is to examine if the Internet users spend more time on the Internet doing conventional or educational activities, rather than nothing or perhaps illicit conducts. Belief in this study examined if Internet users believe and accept the social rules and policies in the community as well as if they respect the institution that enforce the policies. While studying how smoking-related behaviours among youth in China are influenced by knowledge, attitude and other social factors, [24] stated that the tendency of a youth to not adopt a smoking habit all depend on how such youth feel the social pressure from some of their peers or significant others to acquire knowledge about dangers and risks involved in doing such activity and their respective attitude having known the level of dangers involved. For the purpose of this study, Knowledge examined the level of technical capability of Internet users on Internet security mechanism in Nigeria and if they are enthusiastic to acquire more of such knowledge and also examined the attitude of such Internet users if or having acquired such knowledge, how frequent or willing are they to utilize them.

The selection of factors that influence Internet crime raises the question of whether social factors address some issues such as the need for getting users to behave in the way that the security measures require. A disparity between expected and actual user behaviour can occur as a result of either of two factors. Even though security measure consist of social and technical systems that has both technical and social components respectively, some security design methods do not address human factors. This may result in design decisions that do not consider the needs and requirements of social aspects of the system. The ideal approach actively seeks to incorporate social needs into the security design method, thereby improving the overall Internet system design. Without a framework describing these factors and their significance during the practical application, it is difficult to know why or how the proposed Internet security solution is effective. There is therefore a need to identify the type and significance of the social factors that influence Internet crime in order to improve it, and inform future research efforts into Internet security system development. Proper security measures consist of coordinated steps which are both technical as well as social factors, taken to ensure maintenance and provision of high levels of Internet security within an organization or community.

A security culture taken from a human dimension is an important component in the security measures that an organization has adopted. This culture consists of all the social and cultural steps adopted to properly analyse how they influence the Internet security system [25]. Therefore, the building blocks of a secure Internet environment not only consists of technical measures but also social factors that influence the Internet security and they include people and the Internet security culture. Reduction of security threats and incidents can be achieved through a social approach which consists of instilling a culture of security through initiatives such as security awareness through imparting the Internet users with more knowledge and skills. This reinforces the technical skills and measures that an organization may have put in place to boost Internet security [25]. The knowledge and skills already acquired by or imparted to the users are important as they enable them to act appropriately when handling Internet and its resources by applying a pattern of human activities that boost Internet security. Furthermore, Internet crime can be influenced by social factors such as attitudes and beliefs which mould individual behaviour. These attitudes and beliefs manifest themselves in the behaviour of the Internet users and they get imprinted in the activities they perform on a daily basis including in the environment where they are accessing the Internet [25]. Positive behaviour contributes to proper adoption of technical measures due to desirable attitudes and beliefs being imprinted in operations that users perform when using the Internet. Although technical knowledge is important, its effectiveness largely depends on the social behaviour and attitudes of the people who are using the Internet. The motivation, level of knowledge, available training and willingness in performing duties in a secure environment usually make the difference in the adoption and compliance of the security measures and policies available respectively [26].

4. RESULTS AND DISCUSSION:

Based on the theoretical perspectives discussed above, the highlighted social factors that potentially have impact on Internet crime are discussed below:

4.1 Security Policy:

In respect to the GDT earlier mentioned in this study, it is an established fact that security policies are tremendously important in mitigating Internet attacks on Internet users [7]. Security policies can be in different forms, but majorly, it is widely defined as any enactment by relevant governmental agencies that protect Internet users'

activities and information sharing. Security policy also entails the responsibility of guiding users Internet usage, provide rules, guidelines on how the Internet can be used properly and in a secure way such that the users are not vulnerable to Internet attacks and make the misuse of Internet illegal and punishable crime [18]. Previous researchers have provided inconsistent findings on the role of security policy and how it influences Internet security management. For instance, [18] found the establishment of security policy to be significantly efficient in preventing the misuse behaviour of Internet by serving as a deterrent mechanism for trespassers. Similarly, [27] found security policy as a significant antecedent variable to Internet users' safety on the Internet. In line with this, [28] justified that the provision of stern security policy is part of the social factors that influence Internet crime in Nigeria. The study strongly recommended policy makers to enact stern policies that discourage the misuse behaviour of Internet technology and discourage Internet crime in Nigeria. Contrary to those findings, [22] found no significant effect of security policy on users' misuse behaviour of the Internet.

[29] insisted that there is a convincingly huge relationship between security consciousness and Internet usage. The author emphasizes that security policies are important in ensuring safety and protecting users and users' information sharing on the Internet. Additionally, enacting security policies by governmental agencies is not enough measure to eradicate Internet crime. Agencies must also make sure to notify users of the policies and ensure the terms of the security policies are understandable and comprehensible by Internet users. In the same vein, [30] added that the lucidity and widespread promotion of security policies influence Internet users' adherence to security policies. In other words, enacting Internet security policies that protect Internet users is as important as making the policies accessible, understandable and comprehensible. Agencies should also be responsible for making Internet users aware of the terms and conditions of security policies because users awareness of security policies determines their compliance and subsequently affect their safety and protection on the Internet [31]. In view of the above findings reported in extent literatures, the GDT supported the two major facts that; how the perpetrators perceived the severity of security policies imposed by the government or organization and how they perceived the certainty of such security policies being implemented will have a direct influence on such users intention to violate or getting involved in Internet crime. Hence the following hypotheses were proposed:

H1: Perceived certainty of security policy has influence on Internet crime in Nigeria.

H2: Perceived severity of security policy has influence on Internet crime in Nigeria.

4.2 Attachment:

In respect to [6] theory that stated that an individual is likely to be involved in a criminal activity when he/she has a weak or entirely lack social bond, that serves as a control mechanism which can prevent them from engaging in such act. Attachment is first of the four factors proposed by this theory that social bonds rely on. [21] stated that if a person feels attached to their organization more (and for the purpose of this study, Nigeria as a community), there is high tendency that they will not intend to get involved in any criminal activities. [22] argued that attachment can exist in different forms based on how the theory is intended to be applied, it could be parental attachment which involved being attached to one's parent, school attachment which involved being attached to one's academic institution, organizational attachment which involves being attached to one's place of work or community attachment which entails being attached to one's community as a whole, which is mostly applicable to the purpose of this study. [32] mentioned that lack of attachment means lack of respect. In general, that means an individual lacking respect for the community is prone to get involved in criminal activities, thus violating the rules and policies of such community or organization. [32] further argued that attachment is not limited to respect for community alone, it is also about being attached to moral authority in general. Consequently, attachment, being one of SBT factors, can also be viewed as a factor that has a direct influence on Internet crime in Nigeria. [23] also describes attachment as recognition with societal values. From above findings, this study proposed:

H3: Attachment has a direct influence on Internet crime in Nigeria.

4.3 Commitment:

As the second factor in SBT, commitment plays a significant role in assessing a person criminal activities intention. [21] argued that if people are involved in conservative or socially accepted activities, they have a lower tendency of being engaged in any criminal activities because they will be too busy spending time with conventional people. [20] explains that individuals are the fundamental issue in the human parts of information security, because of their immediate contact with information. Their obligation and sense of duty regarding protecting information resources assume an imperative role in this aspect. Commitment denotes the desire to secure a high standard occupation. Individual accomplishment and status are quite essential to committed people [7]. They invest additional time and vitality keeping in mind the end goal to make progress in their professions. A committed individual would not want to get involved in activities that can put their career and reputation in jeopardy [22]. Subsequently, workers with greater commitment to their organization are less inclined to violate the security policies. Consequently, based on the above studies, an individual that is commitment to his/her community will totally deter from getting engaged in Internet crime, and this study thus proposed another hypothesis that:

H4: Commitment has a direct influence on Internet crime in Nigeria.

4.4 Involvement:

Based on the SBT, involvement plays equally an essential role as regards to previously mentioned factors, when analysing human criminal intention or capability. [23] describes involvement as creating or developing a good relationship with people or colleagues. [5] also demonstrated that the tie of involvement or participation such as attending informal meetings with people, creating personal relationships, being loyal and faithful to the organization and community are efficient in reducing computer abuse by the workers.

[33] argues that involvement can be identified with costs of opportunity and how individuals invest their time. In particular, [6] took advantage of the old viewpoint that "idle hands are the devil's workshop" in that if individuals are investing their time occupied with some type of conventional action, at that point they are not, by definition, investing their time occupied with antisocial movement. For instance, young people who are intensely associated with lawful school-related exercises, either scholastically, socially, or physically, won't invest that same time obliterating property, stealing people's belongings, injecting heroin, and so on. This isn't to state, obviously, that such youth can't take part in those practices prior or after their lawful exercises. Nonetheless, Hirschi contended that, in the course of that event, such person won't be involved in criminal acts [33]. In respect to the aforementioned studies, Internet users regular involvement in conventional activities can deter them from getting involved in Internet crime, thus this study proposed hypothesis that:

H5: Involvement has a direct influence on Internet crime in Nigeria.

4.5 Belief:

Belief is the last type of social bond distinguished by [6] and it denotes how much one abides by the qualities related with conducts that adhere to the law; the presumption being that the more critical such esteems are to a man, the more improbable he or she is to take part in criminal/degenerate conduct. For instance, young people who don't regard the thought that it is a terrible plan to be absent from school, and rather regard spending the day playing musical, computer game and utilizing unlawful drugs will probably do only that. On the other hand, young people who, for instance, share the conviction that utilizing unlawful drugs is not right are less inclined to take part in such conduct. Despite the fact that this relationship is very basic, the hidden idea Hirschi was taking advantage of was that there is a critical connection amongst opinion and conduct, not specifically that opinion inspire individuals to carry out criminal act, yet rather that pro-social sentiments oblige individuals from carrying out the violations they generally would have without such belief social bonds [33]. [20] stated that belief, also known as personal norms denotes the workers' esteems and perspectives on information security conformity with organizational policies. [22] researched the role of belief in the development of appropriate computer behaviour. An appraisal of the study uncovered that belief influence people's disposition towards participating in organizational information security misconduct [20]. It is guessed that people with good individual esteems and standards have an uplifting disposition towards agreeing to information security policies in organizations [20]. Similarly, having a proper and positive personal norms and belief has a direct influence on Internet crime in Nigeria, hence the hypothesis that:

H6: Belief has a direct influence on Internet crime in Nigeria.

4.6 Attitude:

As previously discussed in this study, and evidently supported with the technology acceptance model that attitude is a social factor which this study examined on how it influence Internet crime in Nigeria. Internet users' willingness to abide by Internet security policies affects the effectiveness of those policies and regulations. Few studies have also argued in the similar direction. For instance, [31] presented empirical evidence on the significance of Internet users' compliant behaviour. Their findings imply that users' behaviour to comply with security guidance affects their protection and safety on the Internet. In other words, Internet users' consciousness and knowledge of the fact that the Internet can be misused and how much a user is aware of the fact that the Internet has the potential of anchoring scores of Internet crime reduce their vulnerability. This knowledge basically makes users become wary of surfing aimlessly on the Internet and influence their compliance to implementing the available technical measures in protecting their activities on the Internet. A study conducted by [34] gave empirical backings to this contention by emphasizing that Internet users' attitude towards accepting and adopting security measures for protecting their respective selves from Internet attacks generally have a significant influence on Internet crime. Similarly, the work of [35] empirically justified the fact that Internet users' intention to comply with security guidance on Internet security and to behave responsibly with regards to computer security is influenced by certain factors which include their attitude and willingness to comply to the security measures. Therefore, this study hypothesized that:

H7: Internet users' attitude has a direct influence on Internet crime in Nigeria.

4.7 Knowledge:

In reference to the social cognitive theory mentioned earlier, that validated knowledge as an informal social factor, whose influence on Internet crime in Nigeria was examined in this study is to give room for proper understanding of what knowledge stands for. Knowledge in this sense refers to the technical know-how of Internet users on how to implement security measures like antivirus software, firewall, anti-malware software, spam filter, managing web browser settings, password management, file sharing and protection. Internet protocol securities and so on are part of the features that play important role on the effectiveness of security measures. As such, [36] gave an account of a considerable relationship between users' computer skills and Internet security. Similarly, [37] found users' computer skills to be significantly related to the use of anti-spyware software as a preventive measure of cyber-attack. [38] also provided an empirical justification on the importance of users' technical know-how preventing Internet crime and other mischievous attacks on the Internet. Similarly, [39] found a considerable relationship between knowledge, users experience and positive security behaviour of Internet users. In accordance with the findings from previous studies, this study hypothesized thus:

H8: Internet users' knowledge has a direct influence on Internet crime in Nigeria

5. CONCLUSION:

Discussed in this paper is conceptual modeling of social factors using social control. The work of [7] was adapted for the conceptual model. The conceptual model differs from the original work of [7] in the area of social pressure; while subjective norm and co-worker behaviour formed the two social pressure found under the informal control work of [7], the conceptual model categorised attitude and knowledge under social pressure as informal control. The essence of conceptual model is to show the connections between the social factors that are considered as the determinants that influence Internet crime. Although, the connections of the variables were hypothesized but not tested and therefore, left as future work. Integrating GDT and SBT to assessing human compliance intention is not a common undertaking, but few scholars have done this in past studies with positive outcomes; that was why this study adopted such procedure in examining Internet crime in Nigeria.

Deducing from the theoretical arguments and reviews of past relevant studies, this study has found that social variables extensively play a vital role in tackling Internet criminals and their offensive activities. This study integrated two theories that are well established in social control perspective to understand how social factors influence Internet crime in Nigeria and to also propose a model showing the relationship to support the study. The adopted theories are SBT and GDT coupled with informal control social factors such as attitude and knowledge. The social variables that were theoretically adopted from the GDT are certainty and severity in relative to security policy as a formal control social factor. While on the other hand, the whole four factors of the SBT that were adopted are: (1) attachment (2) commitment (3) involvement (4) belief. The impacts of these variables on Internet crime in Nigeria were examined. In respect to [7] studies, that stated that, in other to effectively evaluate human compliance or behavioural intention, two social control methods need to be applied; therefore, the two social control methods, which are: (1) formal (2) Informal control system, were applied in this work. The formal control was basically stressed to be a control system that involved regulatory institution, organization, or perhaps the government for the purpose of this study. And in other to implement such control system to influence people's behaviour, it was revealed that it needs to be imposed in form of sanctions or penalties against any criminal acts; these sanctions are to clearly specify the unacceptable behaviours from the people which will then influence how they perceive threat of the penalty. The effect of socially acceptable moral standards on humans' behaviour is a reflection of informal control system [7].

REFERENCES:

1. Bandura, A. (1988). Organisational Applications of Social Cognitive Theory. Australian Journal of Management, 13(2), 275–302. https://doi.org/10.1177/031289628801300210
2. Martin, C. A., Rivera, D. E., Riley, W. T., Hekler, E. B., Buman, M. P., Adams, M. A. and King, A. C. (2014). A Dynamical Systems Model of Social Cognitive Theory. IEEE American Control Conference, 2407–2412. https://doi.org/10.1109/ACC.2014.6859463
3. Yoon, H. J., and Tourassi, G. (2014). Analysis of online social networks to understand information sharing behaviors through social cognitive theory. Proceedings of the 2014 Biomedical Sciences and Engineering Conference, 1–4. https://doi.org/10.1109/BSEC.2014.6867744
4. Straub, Detmar and Welke, Richard. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision Making," MIS Quarterly, (22: 4).
5. Theoharidou, M., Kokolakis, S., Karyda, M. and Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799.Computers and Security, 24(6), 472–484. https://doi.org/10.1016/j.cose.2005.05.002
6. Hirschi, Travis (1969). Causes of Delinquency. Berkley: University of California Press.

7. Cheng, L., Li, Y., Li, W., Holm, E. and Zhai, Q. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. Computers and Security, 39(PART B), 447–459. https://doi.org/10.1016/j.cose.2013.09.009
8. Ross, E. A. (1896). Social Control. American Journal of Sociology, 1(5), 513–535. https://doi.org/10.1086/210551
9. Jiang, S., Wang, J. and Lambert, E. (2010). Correlates of informal social control in Guangzhou, China neighborhoods. Journal of Criminal Justice, 38(4), 460–469. https://doi.org/10.1016/j.jcrimjus.2010.04.015
10. Jiang, S., Lambert, E. G., Saito, T. and Hara, J. (2012). University Students' Views of Formal and Informal Control in Japan: An Exploratory Study. Asian Journal of Criminology, 7(2), 137–152. https://doi.org/10.1007/s11417-012-9126-2
11. Frink, D. D., and Klimoski, R. J. (2004). Advancing accountability theory and practice: Introduction to the human resource management review special edition. Human Resource Management Review, 14(1), 1–17. https://doi.org/10.1016/j.hrmr.2004.02.001
12. Datta, A., Kar, S., Sinopoli, B. and Weerakkody, S. (2016). Accountability in cyber-physical systems. 2016 Science of Security for Cyber-Physical Systems Workshop, SOSCYPS 2016. https://doi.org/10.1109/SOSCYPS.2016.7579998
13. Boos, D. and Grote, G. (2012). Designing controllable accountability of future Internet of things applications. Scandinavian Journal of Information Systems, 24(1), 3–28.
14. Dubnick, M. (1998). Clarifying Accountability: An Ethical Theory Framework. Public Sector Ethics: Finding and Implementing Values, (609), 68–81. Retrieved from http://scholars.unh.edu/polisci_facpub/46/
15. Jagadeesan, R., Jeffrey, A., Pitcher, C. and Riely, J. (2009). Towards a theory of accountability and audit. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5789 LNCS, 152–167. https://doi.org/10.1007/978-3-642-04444-1_10
16. Goodhue, D. L. and Straub, D. W. (1991). Security concerns of system users. Information & Management, 20(1), 13–27. https://doi.org/10.1016/0378-7206 (91)90024-V
17. Schuessler, J. H. (2009). General deterrence theory: Assessing information systems security effectiveness in large versus small businesses. Retrieved from http://proxy2.hec.ca/login?url=http://search.proquest.com/docview/304962568?accountid=11357%5Cnhttp://gutenberg.hec.ca:3210/sfxlcl3?url_ver=Z39.882004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&genre=dissertations+&+theses&sid=ProQ:ProQuest+Dissertations
18. D'Arcy, J., Hovav, A. and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. Information Systems Research, 20(1), 79-98.
19. Straub, D. W. (1989). Validating Instruments in MIS Research. MIS Quarterly (13) 2, pp. 147-169.
20. Safa, N. S., Von Solms, R. and Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. Computers and Security, 56:70–82.
21. Lee, J. and Lee, Y. (2002). A holistic model of computer abuse within organizations. Information Management and Computer Security, 10(2), 57–63. https://doi.org/10.1108/09685220210424104
22. Lee, S. M., Lee, S. G. and Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information Management, 41(6), 707-718.
23. Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information and Management, 51(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001
24. Xu, X., Leung, D. Y. P., Li, B., Wang, P. and Zhao, Y. (2015). Smoking-related knowledge, attitude, social pressure, and environmental constraints among new undergraduates in Chongqing, China. International Journal of Environmental Research and Public Health, 12(1), 895–909. https://doi.org/10.3390/ijerph120100895
25. Tarimo, C. N., Kuwe, J., Louise, B. and Kowalski, S. (2006). A Social-Technical View of ICT Security Issues, Trends and Challenges: Towards a Culture of ICT Security - The Case of Tanzania.
26. Anderson, Catherine L. and Ritu Agarwal. Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. 2010. Web. 16 June 2017.
27. Haeussinger, F. J. and Kranz, J. J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behaviour. International Conference on Information System 2013, 1-16.
28. Odumesi, J. O. (2014). Combating the menace of cybercrime. International Journal of Computer Science and Mobile Computing, 3(6), 980-991.
29. Chan, M., Woon I. and Kankanhalli A. (2005). Perceptions of information security at the workplace: linking information security climate to compliant behavior," Journal of Information Privacy and Security, 1(3), 18-41.
30. Siponen, M., Mahmood, M. A. and Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? Communications of the ACM 52(12), 145-147.

31. Herath, T. and Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 1-12. Available from: http://www.swdsi.org/swdsi05/Proceedings05/paper_pdf/An%20Examination%20of
32. Travis Hirschi. Causes and Prevention of Juvenile Delinquency. Sociological Inquiry, Wiley Online Library, Volume 47, Issue 3-4, 1977.
33. Pratt, T. C., Franklin, T. W. and Gau, J. M. (2008). Key Idea : Hirschi's Social Bond / Social Control Theory. Key Ideas in Criminology and Criminal Justice, (1969), 55–69. Retrieved from www.sagepub.com/upm-data/36812_5.pdf
34. Siponen, M. and Vance, A. (2010). Neutralization: New insight into the problem of employee information systems security policy violations. MIS Quarterly 34(3), 487-502.
35. Ng, B. Y. and Rahim, M. A. (2005). A socio-behavioral study of home computer users' intention to practice security. Proceedings of the 9th Pacific Asia Conference on Information Systems, Bangkok, Thailand.
36. Frank, J., Shamir, B. and Briggs, W. (1991). Security-related behavior of pc users in organizations. Information and Management 21(3),127-135.
37. Dinev, T. and Hu, Q. (2007). "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies," Journal of the Association for Information Systems: Vol. 8 : Iss.7, Article 23. Available at: https://aisel.aisnet.org/jais/vol8/iss7/23.
38. Gaston, S. J. (1996). Information security: Strategies for successful management, Toronto: CICA Publishing.
39. Rhee, H. S., Kim, C. and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior, Computers & Security, 28(8), 1-11.