Invited Paper: Employee Emancipation and Protection of Information

Yurita Abdul Talib and Gurpreet Dhillon
School of Business, Virginia Commonwealth University
301 W Main Street, Richmond, VA
{abdultalibyy, gdhillon} @vcu.edu

***Abstract*—Incidents of computer abuse, loss of proprietary information and security lapses have been on the increase. More often than not, such security lapses have been attributed to internal employees in organizations subverting established organizational controls. What causes employees to engage in such illicit activities is the focus of this paper. In particular we argue that increased employee emancipation leads to better protection of information in organizations. In this paper we present our argument by reviewing the appropriate theoretical literature and by developing conceptual clarity of the related constructs.**

I. Introduction

INTERNAL threats from employees have always been acknowledged as a major source of security breaches in organizations [37]. A recent report by privacyrights.org on data breaches indicates a substantial increase of internal security breaches from 2005 to 2009 that involve various cases of stealing personal information of internal publics, co-workers and clients in different organizations such as banking, health, university and government offices. The breaches cause a lot of damage to a company's computer systems, financial data, business operations and ultimately, it's reputation. These events are created by the people who are given privileges to use IS in organizations and subsequently misuse that access privilege. Stanton et al. [32] describe that regardless of users' intent - from naive mistakes to intentional misuse - security breaches because of lack of compliance can be curtailed. The importance of the issue, hence, attaches relative importance of research into insider threats that have consistently focused on employees' compliance behavior to IS policies. IS literature has a long tradition of studying the management roles in cultivating a security culture and its impact on intentions to comply [11][22][31]. The premise of these studies is that management commitment, communication and enforcement of power motivates employees to comply with security policies. For example, a study conducted by Arbodela et al. [4] involving the identification of antecedents of employees' safety compliance behavior discovers that top management commitment to safety was perceived to be an integral determinant of safety culture. Additionally, Chan et al. [11] suggests that upper management practices are found to be positively related to employees' compliance behavior through mediation of perception of information security climate. Along the same lines, Spitzmueller and Stanton [31] reveal that organizational commitment, organizational identification and attitudes towards technology predict employees' intentions to comply with security policies.

An associated stream of research is one that investigates motivation of management through reward and sanction in influencing employees' compliance behavior. An organization that is truly dedicated to security will recognize the need for motivation beyond mere security awareness and will develop an effective security motivation program along with or as a part of a continuing awareness effort. It should employ the most controllable and powerful motivators, rewards and penalties [27]. A study conducted by Siponen et al. [30] finds that sanctions have a significant impact on actual compliance with information security policies. According to Parker [27] penalties or sanctions often involve loss of favor, perks, position, or remuneration. One group manager publicly posted the name of anybody who revealed his or her password and required everyone in the group to immediately change their passwords. This produced peer pressure to keep passwords secret because nobody liked having to learn a new one. However Pahnila et al. [26], commenting on factors that explain employees' IS security policy compliance among Finnish companies, suggest that rewards do not have a significant effect on actual compliance with IS security policy. Most of the prior research in internal control towards security problems deals with protection motivation and cultivating a security culture. While this stream of research is useful, it falls short of suggesting why employees subvert security policies in the first place. Moreover, from an ontological perspective, previous research orientation is dominated by functionalist and interpretivistt paradigms [13]. Although these paradigms are important, information systems security research can also be studied from alternative viewpoints, *viz* critical. Based upon the notion that critical humanist study of information systems security is underdeveloped, we attempt to explain the issue of employees' intention to comply with security policy by arguing that lack of emancipation of an individual is a significant cause for security lapses.

II. WHO IS AN EMANICIPATED EMPLOYEE?

The concept of emancipation was established by Critical Social Theorists (CST) as an alternative to traditional research approaches. The fundamental goal of CST is improvement of human conditions, which takes into account the human construction of social forms of life and the possibility of their recreation [25]. The critical theorists seek to emancipate people; they are concerned with finding alternatives to existing social conditions. More specifically, with emancipation, the organization actors have the capability to transform organizational conditions.

Habermas's Theory of Communicative Action is an extension of CST with a broader notion of rationality. Habermas developed the concept of "communicative action", defined as "the type of interaction in which all participants harmonize their individual plans of action with one another and thus pursue their illocutionary aims without reservation" [16]. According to this perspective, in order to overcome social crises, it is necessary to counterbalance purposive rationality by bringing communicative rationality back into play. Hence the framework highlights the importance of developing a society based on free, undistorted communication in order to prevent colonization and technization of the life and world by power and money [16].

The study of human emancipation has been long established in the field of social studies. And among the well-known studies are those on 'women emancipation' [1][2][8][12][18]21. The term 'women emancipation' is used to denote equalization of opportunity structure in which women are to gain equal status as men as a result of balancing of gender roles [21]. Women now are no longer stuck in the kitchen with baby diapers, but are involved actively in social structures. The prominent benefit of equality of gender is in education, in which for a long time in history, women were not given opportunity to obtain an education. Education opens up many opportunities for women, while eliminating ignorance and silent suffering. Women are now emancipated enough to join the labor force in which they can be found amongst the most powerful politicians, scholars, CEOs of companies and holding many more jobs that were earlier monopolized by men. This movement of equality in gender roles or emancipation allows women to discover their suppressed dignity and potential. Though some proponents of women emancipation see it as a stimulus for crime committed by women and delinquent behaviors, most support the idea as a means of manifestation of democratic ideals.

Hirschheim and Klein [17] purport that "Information systems as social communication systems have potential of freeing employees from repressive social and ideological conditions and thereby contributing to the realization of human need" (p.87), i.e., information systems facilitate emancipation. This notion is supported in information systems that are a basis of poor information access, particularly via traditional method of information dissemination and sharing in a large and distributable organization [9]. However, due to the fact that 'information is power' [35], organizations impose security mechanisms in terms of limiting employees' access to information systems in order to preserve management power. The inequality of power in information access creates oppressed individuals, which significantly contradicts the earlier view that information systems should free employees from oppressive conditions [17].

Given the aforementioned, in this paper we aim to stimulate the idea of employees' emancipation in information access in organizational information systems. Ultimately the central objective is to relate employees' emancipation and their compliant behavior. In cultivating the idea, we base our conception upon the concept of women emancipation, in which managers and employees are given equal right to access an organization's information. The transformation in information sharing and decentralization of power would then dismiss the power structure that alienates the employees and makes it difficult for them to undertake their work and get involved in decision-making processes. Emancipation therefore provides equality between managers and workers, hence allowing for sharing of responsibilities and freedom to take decisions. Responsibility for successful decisions' results in employees becoming more motivated and hence increases their morale and develops a feeling of ownership. In turn, the ownership feeling makes employees feel responsible towards protecting the assets of an organization.

III. HOW EMANCIPATION FACILITATES INFORMATION PROTECTION?

In an information systems environment, there are only a few individuals (usually the management), who have a privileged access to information and hence organizational power. This is usually at the expense of other people in the organization (i.e. employees). Since information is power [35], and only a privileged few have access, it leaves a vast majority as being powerless. Hence the notion that power 'creates' oppressed individuals in which it stops them from carrying out what they would freely choose to do otherwise, is realized [7]. Limiting employees' access to information not only creates inequality of power but also restricts the involvement of the oppressed in the decision making process. Ultimately, these employees get alienated, disgruntled and generally do not feel that they are an active participant in organizational affairs.

Alienation of employees as the result of the power structures can be represented by four dimensions, namely powerlessness, meaninglessness, isolation and self estrangement [33]. Correspondingly, the feelings of powerlessness as a result of being controlled by others and isolation, that leads to a lack of sense of belonging, diminishes the worker's commitment towards the organization [33]. As a result, employees who feel alienated from their employer are less motivated to commit and more likely to take decisions that are unethical. This in turn leads to non-compliance with security policies. A combination of these circumstances makes an organization susceptible to security breaches.

In this paper, the focus of employees' emancipation is towards information access in an organization's information systems. We define emancipation as freeing the employees from the power structure by increasing the scope and depth of their information access. This, we argue, leads to decentralization of power between employees and managers,

which subsequently provides employees with the authority to be involved in the decision making processes. Information sharing is an instrument in eliciting employees' involvement and building trust [19]. Based upon decision making involvement and the culture of trust that an organization creates, it can foster greater emotional buy-in from employees.

As an example, imagine that employees are allowed to share information about financial status during a crisis, at which time the management often hoards and restricts access to such information. However the employees might be able to help with suggestions. Being at the operational level, employees know better as to what specific actions affect the overall business. They are also more likely to offer valuable ideas on how the operations can be improved. Since meaningful suggestions from employees are more likely to be adopted, it builds a situation where the employees feel valued by the organization. That in turns can help build morale, giving employees a greater sense of worth and emotional ownership in the company.

This sense of ownership or buy-in triggers a sense of responsibility for the entity [14]. When employees feel responsible for the entity, they will protect what belongs to the entity - in our case the information systems and information that they handle. This is logically supported by the assertion that 'rational' people will not destroy or take unnecessary action against something that belongs to him. As much as possible these people will protect what they are responsible for. This assertion is fundamental to our argument that emancipation of employees, by allowing them access to information and participation in the decision making process, leads to a sense of ownership and responsibility. This will form the basis for ensuring complete support and adherence of all employees to organizational security policies.

IV. On the Nature and Scope of "Responsible Behavior" for Information Protection

Employees' sense of ownership towards the information, information systems and hence the organization itself may have a positive impact on employees' behavior. It has been argued that ownership creates a sense of responsibility for an object [14] which initiates behaviors of protecting the owned object [35].

Bear, Manning and Izard [15] purport that responsible behavior in obedience and compliance to a rule entails self-motivation and self-guidance, and is not merely a response to external supervision, rewards and punishment. Hence, prior research on employees' compliance behavior to security policy that focuses on these external factors is not the sole contributor for building responsible behavior in employees'. While embedding these factors, which are merely enforcement of power, is empirically effective, over time their significance will be eroded. These external factors change over time and are impossible for employees to follow because of the constantly shifting direction to conform to the influences [5]. Therefore we believe that the good behavior of the employees on policy compliance is only temporary, if it is present at all.

On the other hand, responsibility behavior of employees, which derives from employees' cognitive and emotional factors [15], would deem to be more effective in shaping their behavior towards compliance. With responsible behavior, people will act accordingly because they perceive that they are the cause of their own behavior, in which case, if they do not comply with the policies, they are responsible for that as well, not the other people or some other external factors. People with a responsible behavior will act the way they should whether anyone is watching or not and also remain aware of the consequences of their behavior for the welfare of others.

In summary, as stated previously, the emancipation of employees allows them to acquire a feeling of ownership towards the organization (object). This is achieved by providing an equality of power in term of information access and consequent involvement in the decision making process. This ownership signifies that both employees and managers are entitled to use and engage with the object, and hence be held responsible by each other in protecting the owned object. Based upon this assumption, we postulate that employees will protect the organization from any harmful acts by performing a 'right' responsible behavior in accordance with organizational security policies.

V. A Conceptual Model of Emancipation and Information Protection

Emancipation refers to freeing employees from oppressive conditions, hence enabling them to realize their full potential [3]. According to Alvesson and Willmott [3], the concept of emancipation in organizations is described as "freeing employees from unnecessarily alienating forms of work in organization" (p.433). Ultimately the central focus of emancipation lies is providing communication discourse in which all level of employees are able to access the same amount of information and are involved with decision making processes, share responsibility and hence promote democracy in organizations. In the same vein Hirschheim and Klein [17] purport that emancipation can be practiced in organization through involvement in decision making process, which in turn reduces the power of management and increases employees' responsibility. Similarly, Sashkin [28] identifies the need for employers to fulfill employees' basic human needs at the workplace for autonomy, meaningfulness of work and decreased isolation. Failure to provide those needs, according to Sashkin [28], is unethical as it creates physiological and physical harm to the employees. In relation to the previous literatures, we propose that while employees' involvement in decision making process is vital, it is not achievable if they are not emancipated in accessing the information. Our argument is based on current practices of an organization in the digital age wherein most information, including that for decision making purposes, are inputs, processed and delivered via vastly controlled computer based information systems. Without substantial and suitably structured access privileges for the information, it is rather difficult for the employees to be involved in and contribute to the process. A summary of our postulated relationships of emancipation and information protection are presented in Figure 1.

Emancipation of individuals has become an increasingly important method of increasing employees' creativity and productivity and researches have directed increased attention towards emancipation effectiveness. Research results consistently contribute to the notion that giving the employees involved in the tasks the authority to take decisions, makes them more creative and motivated to aim for successful production decisions. In a security context, the aim is towards protection of the information, particularly in compliance with security policies. Although previous studies in IS have examined the positive consequences of emancipating employees in information system development, none has made an attempt to study emancipation of employees for access to information. Based on the above, we posit that by emancipating employees with respect to information access, employees are more likely to comply with an organization's security policies directly or indirectly.

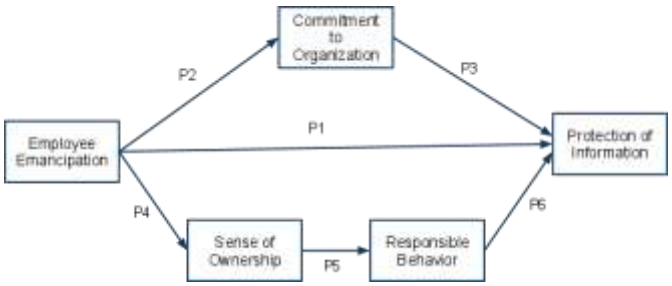

Fig. 1. Conceptualizing employee emancipation and protection of information

As previously mentioned we postulate that emancipation can also have an indirect relationship with protection behavior. One of the indirect routes is its influence on employees' commitment to the organization. Employees' commitment is defined as the feeling of desire, need or obligation to remain in an organization [23]. As employees are given more power towards information access and deliberate decision making authority, it increases their commitment towards the organization. There is support in the literature for this contention, which claims that participation in decision making increases employees' organizational commitment [10][30] whereas alienation of employees from an organization will diminish their commitment [33].

In information systems, the concept of emancipation has largely been investigated within the realm of information systems development (ISD), particularly through the application of both Habermas's Theory of Communicative Action and Critical Social Theory. Cecev-Kecmanovic and Marius [9] address effectiveness of emancipation in their 15 years longitudinal case study of development of Information System for Information Dissemination (ISID) in Colruyt Company in Belgium. They discover that with the amount of increased power given to the employees, they are less alienated and oppressed, leading to increased individual commitment. Similarly Kanungo [20] finds that impact of emancipatory roles of ICT development in rural areas suggests that by involving villagers with the development process, they become more committed towards using the systems. Regardless of the context of the organization, employees' commitment will direct an individual's effort toward achieving organizational goals [24].

Another stream of research, as introduced previously, studies the achievement of an organization's security goals through a sense of ownership and responsible behavior. Previous studies provide substantial evidence that employees' involvement in decision making process creates a stronger sense of ownership or identity [6][29]. With the empowerment of being involved in decision making process, employees will be able to contribute more valuable ideas to improve operations since they are attached directly at the operational level. Subsequently, their meaningful suggestions are more likely to be accepted and adopted. This in turns strengthens motivation by providing employees with the opportunity to attain intrinsic rewards from their work, such as a greater feeling of being valued. This helps in inculcating and increasing a sense of ownership towards the organization.

Our definition of sense of ownership is borrowed from van Dyne and Pierce [34] which defines it as "psychologically experienced phenomenon in which an employee develops possessive feelings for the target" (p. 439). The feeling of ownership makes the employees feel they own the organization, in other words- they have a feeling that the organization belongs to them, which is fundamentally different from the feeling of their need to remain in an organization or organizational commitment [34]. If employees feel that they are part of the business processes, they become much more attached to their work. As a result employees become more conscientious of their work and how it affects the organization. Thus, the feeling of ownership initiates a sense of responsibility for the entity [34].

Being responsible, according to Bear et al. [15], means the ability to take decisions that are morally and socially right. This conveys the notion that employees will act accordingly because they realize that they are accountable for their own behavior, regardless of whether they are being monitored or not. Bear et al. [15] contend that responsible behavior that is derived from social cognition and individual emotion is more important than responsible behavior constituted by external

TABLE I
PROPOSITIONS POSTULATING RELATIONSHIPS BETWEEN EMANCIPATION AND INFORMATION PROTECTION

Proposition	Description
1	Emancipation will positively influence information protection, both directly and indirectly through affective commitment, sense of ownership and responsible behavior.
2	Emancipation is positively associated with employee commitment to an organization
3	Employee commitment to an organization is positively associated with employee protection of information
4	Emancipation is positively associated with an employee's sense of ownership / belonging leading to information protection
5	Employee's sense of ownership / belonging is positively associated with responsible behavior leading to information protection
6	Employee responsible behavior is positively associated with protection of information

factors. In their study, they gather evidence on how responsible behavior of a student not only benefits the individual but also the members of a school community. The behavior promotes positive effects such as academic achievement and self-worth. Motivated from this notion, we argue that employee's feelings and thoughts (sense of ownership / feeling of being valued /feeling of importance) are the primary determinants that explain how individuals become responsible employees. Embedded responsible behavior influences them to promote positive attitude such as protection of information. A summary of our propositions, as discussed in this section are presented in Table I.

VI. Conclusion

In this paper we have introduced the concept of employees' emancipation and its relationship with organizational commitment, sense of ownership, responsible behavior and protection of information within an organization. While many researchers have commented on an employees' behavioral compliance with security policies and laws and regulations, our research introduces fresh insight by establishing a relationship between emancipation and information protection. Rather than be enshrouded in positivist or interpretivist conceptions, in this research we introduce a critical theorist orientation for the study of information protection. We have argued that protection of information in an organization is influenced by the human cognitive and emotional feelings of individuals, which are derived from the emancipation of an employee from organizational power structures that govern information access. Hence, this paper lays a foundation for further theoretical and empirical research on the protection of information.

References

[1] F. Adler, *Sisters in Crime: The Rise of the New Female Criminal*. New York: McGraw-Hill. 1975

[2] F. Adler, "The interaction between women's emancipation and female criminality: a cross-cultural perspective", *International Journal of Criminology and Penology*, 5, 1977, 101-112, 1977.

[3] M. Alvesson and H. Willmott, "On the Idea of Emancipation In Management And Organization Studies", *Academy of Management Review*, 17(3), 432-464, 1992.

[4] A. Arboleda, P.C. Morrow, M. R. Crum, and S.C. Mack, "Management Practices as Antecedents of Safety Culture within The Trucking Industry: Similarities And Differences By Hierarchical Level", *Journal of Safety Research* 34, no. 2: 189-197, 2003.

[5] A. Bandura, "Social cognitive theory: an agentic perspective", *Annual Review Of Psychology*, *5*21-26, 2001.

[6] B. Benkhoff, "Ignoring Commitment Is Costly: New Approaches Establish the Missing Link Between Commitment and Performance", *Human Relations*, *50*(6), 701-726, 1997.

[7] K. Booth, "Security and emancipation", *Review of International Studies*, 17(4), 313-26, 1991.

[8] S. Box & C. Hale, " Liberation/emancipation, economic marginalization, or less chivalry: The relevance of three theoretical arguments to female crime patterns in England and Wales, 1951–1980", *Criminology: An Interdisciplinary Journal*, *22*(4), 473-497, 1984.

[9] D. Cecez-Kecmanovic, M. Janson & A. Brown, "The rationality framework for a critical study of information systems", *Journal of Information Technology (Routledge, Ltd.)*, *17*(4), 215-227, 2002.

[10] A.L. Pearson and C. Duffy, "Contexts Commitment and Job Satisfaction: A Study in Australian and Malaysian Nursing The Importance of Job Content and Social Information on Organizational", *Asia Pacific Journal of Human Resources* 1999; 36; 17, 1999.

[11] M. Chan, I. Woon and A. Kankanhalli "Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior", *Journal of Information Privacy & Security* 1, no. 3: 18-41, 2005.

[12] R. Deming, *Women: the new criminals.* Nashville: Thomas Nelson, 1997.

[13] G. Dhillon and J. Backhouse, "Current directions in IS security research: towards socio-organizational perspectives", *.Information Systems Journal*, *11*(2), 127, 2001.

[14] L. Furby, "Possession in humans: an exploratory study of its meaning and motivation", *Social Behavior and Personality*, 6, 49–65, 1978.

[15] G.G. Bear, M. A. Manning & C. E. Izard, "Responsible Behavior: The Importance of Social Cognition and Emotion", *School Psychology Quarterly*, *18*(2), 140-157, 2003.

[16] J. Habermas, *The theory of communicative action*, Volume 2. Boston, MA. Beacon Press, 1987.

[17] R.A. Hirchheim, and H.K. Klein, "Realizing emancipatory principles in information systems development: The Case for ETHICS", *MIS Quarterly*, 18(1), 83-109, 1994.

[18] J. James and W. Thornton, "Women's Liberation and The Female Delinquent", *Journal of Research in Crime & Delinquency*, *17*(2), 230, 1980.

[19] G. M. Kandathil and R. Varman, "Contradictions of Employee Involvement, Information Sharing and Expectations: A Case Study of an Indian Worker Cooperative", *Economic and Industrial Democracy* 28(1): 140-174, 2007.

[20] S. Kanungo, "On the emancipatory role of rural information systems", *Information Technology & People*, *17*(4), 407-422, 2004.

[21] S. Karstedt, "Emancipation, Crime and Problem Behavior of Women: A Perspective from Germany", *Gender Issues*,*18*(3), 21, 2000.

[22] K.J. Knapp, T.E. Marshall, R.K. Rainer and F.N. Ford, "Information security: management's effect on culture and policy", *Information Management & Computer Security* 14, no. 1: 24-36, 2006.

[23] J. Meyer and N. Allen, *Commitment in the workplace: Theory, research, and application*. Thousand Oaks, CA US: Sage Publications, Inc. 1997.

[24] J. Meyer and C. Smith, "HRM Practices and Organizational Commitment: Test of a Mediation Model", *Canadian Journal of Administrative Sciences (Canadian Journal of Administrative Sciences)*, *17*(4), 319-331, 2000.

[25] O.K. Ngwenyama, "The Critical Social Theory Approach to Information Systems: Problems and Challenges," in *Information Systems Research: Contemporary Approaches and Emergent Traditions*, H,E, Nissen, H, Klein, and R, Hirschheim (eds,), North-Holland, Amsterdam, pp. 267-278, 1991.

[26] S. Pahnila, M. Siponen and A. Mahmood, "Employees' Behavior towards IS Security Policy Compliance", *Proceedings of the 40th Hawaii International Conference on System Sciences 2007*.

[27] D.B. Parker, "Motivating the Workforce to Support Security", *Risk Management (00355593)* 50, no. 7: 16-19, 2003.

[28] M. Sashkin, "Participative management remains an ethical imperative", *Organizational Dynamics* 14, no. 4: 62-75, 1986.

[29] B. Scott-Ladd, A. Travaglione and V. Marshall, "Causal inferences between participation in decision making, task attributes, work effort, rewards, job satisfaction and commitment", *Leadership & Organization Development Journal*, *27*(5), 399-414, 2006.

[30] M. Siponen, S. Pahnila and A. Mahmood, "New Approaches for Security, Privacy and Trust in Complex Environments*", IFIP International Federation for Information Processing*, Volume 232, 133–144, 2007.

[31] C. Spitzmüller and J.M. Stanton, "Examining employee compliance with organizational surveillance and monitoring", *Journal of Occupational & Organizational Psychology* 79, no. 2: 245-272, 2006.

[32] J.M. Stanton, K.R. Stam, P. Mastrangelo, and J. Joiton, "Analysis of end user security behaviors", *Computers & Security* 24, no. 2: 124-133, 2005.

[33] G. Tonks and L. Nelson, "HRM: A Contributor To Employee Alienation?" *Research & Practice in Human Resource Management*, *16*(1), 1-17, 2008.

[34] L. van Dyne and J. Pierce, "Psychological ownership and feelings of possession: three field studies predicting employee attitudes and organizational citizenship behavior", *Journal of Organizational Behavior*, *25*(4), 439-459, 2004.

[35] S. Zuboff, *In the Age of the Smart Machine*. New York, Basic Books, 1984.

[36] A. Melek and M. MacKinnon. (2006). Deloitte global security survey. [Online]. Available: http://www.deloitte.com/dtt/cda/doc/content/us_fsi_150606globalsecuritysurvey(1).pdf