Knowledge Transfer in Information Security Capacity Building for Community-Based Organizations

Janine L. Spears, DePaul University, Chicago, IL, USA

Tonia San Nicolas-Rocca, School of Information, San Jose State University, San Jose, CA, USA

ABSTRACT

Community-based organizations (CBOs) in the health and human services sector handle very sensitive client information, such as psychiatric, HIV testing, criminal justice, and financial records. With annual revenue often in the range of $1 to $10 million, these organizations typically lack the financial, labor, and technical resources to identify and manage information security risks within their environment. Therefore, information security risk assessments were conducted at CBOs as part of a university service learning course intended to ultimately improve security within participating CBOs. Knowledge transfer between trainees and trainers is essential in order for security improvements to be realized. Therefore, this paper constructs a theoretical model of knowledge transfer that is used as a lens through which to examine initial study results of the CBO interventions as part of an exploratory study.

Keywords: *Capacity Building, Community-Based Organizations, Extrinsic Motivation Service Learning User Participation, Information Security, Knowledge Transfer, Risk Assessment, User Participation*

INTRODUCTION

Nonprofit organizations provide a range of health, educational, welfare, and cultural services to meet societal needs. For example, nonprofit organizations in the health and human services provide foster care and other services for at-risk youths, behavioral health services, HIV/AIDS testing, work training programs, and transitional housing assistance. In short, these nonprofit organizations provide a safety net for society, filling in the gap of addressing societal needs in areas the private and government sectors are not structurally or otherwise feasibly able to carry

DOI: 10.4018/IJKM.2015100104

out (Berman, 2010). Such organizations are often located in low-income communities where their services are accessible to those in need (Minzner et al., 2014).

Given the nature of their respective missions, community-based organizations (CBOs) typically handle very sensitive client information, such as detailed psychiatric records of parents with children living in a children's home; felony records of clients transitioning back into the work force; financial and mortgage records of clients at risk of home foreclosure; alcohol and substance abuse and other mental health records. Intuitively, these data are far more sensitive than credit card information from U.S. bank accounts: if credit card information is accessed by unauthorized parties, the banks will typically bear any associated loss. However, if behavioral or mental health information is compromised, significant reputational, and indirectly, financial loss may occur. Indeed, some state governments classify drug and substance abuse, mental health, and HIV/AIDS data as "super" electronic protected records (Pennsylvania eHealth Partnership Authority, 2015). Given the sensitivity of the data handled by CBOs, and the state and federal regulations that serve to protect these data, it is crucial that CBOs do due diligence in preserving the confidentiality, integrity and availability of the data with which they have been entrusted.

While CBO management may intuitively realize the need for data protection, they generally do not have the resources (i.e., staff, technical expertise, or funding) to assess information security risk, implement security safeguards, or train staff on information security. For example, in a study that surveyed 78 individuals working for nonprofit organizations in Chicago and Southern Illinois with average annual budgets of $1.3 million, Imboden et al. (2013) found that only 56% of respondents indicated their organization had an information security policy, while 67% reported being aware of their organization having at least one information security incident. Non-profit organizations within the study sample that had larger budgets were more likely to have a security policy.

Capacity building initiatives, funded by external entities, are intended to help CBOs fill managerial gaps by providing some intervention intended to help develop infrastructures that aid in sustaining and growing their organizations. Capacity building is defined as "training and educational activities that aim to build the management skills of staff or focus on organizational processes that are necessary to promote growth and demonstrate effectiveness" (Sobeck, 2008). The breadth of capacity building projects is wide and has included implementations of financial controls, policies and procedures related to staffing and governance, grant-writing, strategic planning, and program evaluation (Minzer et al., 2014; Sobeck, 2008; Wetta-Hall et al., 2004). Outcomes studied have included written strategic plans, written and implemented program evaluation mechanisms, new funding source identification, increased grant submissions, and expanded program services (Minzer et al., 2014; Sobeck, 2008; Wetta-Hall et al., 2004). Examples of capacity building activities include information and education sessions, coaching, and technological assistance tailored to the organization (Sobeck, 2008; Kindred & Petrescu, 2015). Private foundations, as well as local, state, and federal governments typically fund capacity building initiatives. Universities also participate in capacity building initiatives, for example, acting as an intermediary between government funders and CBO recipients. In such arrangements, the university develops and administers the capacity building initiative in response to a request for proposal issued by a government funding agency (Kindred & Petrescu, 2015).

Given the sensitivity of client information maintained by CBOs in health and human services, coupled with their gaps in financial, technical, and labor resources, it is suggested here that capacity building initiatives are needed in information security risk management (ISRM). CBOs need knowledge on security vulnerabilities and threats specific to their organizational operations, as well as knowledge on how to manage those risks, given their limited resources. Thus, one objective of an ISRM capacity building program is to provide participating CBOs with

knowledge on information security risks identified within the organization. For example, knowledge on organizational security risks may be gathered from interviews, facility walk-throughs, policy reviews, questionnaires, etc. The second objective of an ISRM capacity building program is to train participants on how their organization's information security can be improved, based on identified risk. The intended program outcome is for CBOs to act on the knowledge gained by taking action to strengthen information security practices. Thus, our research question is: *What are the factors influencing knowledge transfer in an information security risk assessment intervention, and does knowledge transfer result in improvements in information security within participating community-based organizations?*

There is a dearth of research on the information security behavior of CBOs, which is an important research gap given that CBOs are often prone to handling very sensitive client information as part of their organizational missions. Second, while there has been research on capacity building initiatives to strengthen managerial, funding, and financial controls within nonprofit organizations, the present authors are unaware of research on capacity building in ISRM. Third, the literature on knowledge management and information security has presented a need for additional research in this area (Jennex & Durcikova, 2014; Rodriguez & Edwards, 2014). Fourth, the literature on security training programs has highlighted the need for research on training program evaluation. Thus, the present research makes a contribution by proposing an approach to increasing information security knowledge in CBOs, and by evaluating the effects of knowledge transfer during a capacity building intervention on an organization's subsequent security activity. More simply, the study examines whether training efforts meet the objective of strengthened security practices.

The remainder of the paper is organized as follows. First a review of knowledge transfer is presented, along with a set of theoretical propositions. Next, a theoretical model is presented that is then used as a lens through which to examine the results of a qualitative exploratory study. Based on these results, quantitative measures for each construct in the theoretical model are then proposed. Finally, the paper concludes with research implications, plans for future research, and a conclusion.

KNOWLEDGE TRANSFER AS A MEANS TO STRENGTHEN INFORMATION SECURITY RISK MANAGEMENT

Knowledge transfer plays a key role in the success of a capacity building intervention. According to Ko et al. (2005), knowledge is taken to be transferred when learning takes place and when the recipient understands the intricacies and implications associated with that knowledge so that he or she can apply it. For example, a university collaborator may transfer knowledge about security risk to a CBO recipient. Provided the CBO recipient understands the risk explained and what is needed to manage the risk, he or she will be enabled to implement appropriate security safeguards.

As described in San Nicolas-Rocca et al. (2014), knowledge transfer is influenced by absorptive capacity, motivation, user participation, and communication. The present paper builds on that work by examining knowledge transfer in a different context: capacity building within community-based organizations. Moreover, the present study examines whether participating CBO members take action to implement security improvements based on knowledge transferred during a capacity building intervention.

Propositions

User Participation

In a capacity building intervention, user participation is essential. Indeed, research has found that when users participate in ISRM activities, security safeguards were more aligned with business objectives and were more effectively designed and performed within the organization (Spears & Barki, 2010). Therefore, while it is valuable to have IT staff participate in capacity building interventions, it is suggested here that organizational capability in ISRM will be particularly effective if system users participate. User participation in capacity building within CBOs is particularly important, given the limited (if any) full-time IT staff in CBOs. Thus, the present study is focused on user participation in capacity building interventions. Given its cognitive effects and the positive outcomes previously found from user participation in ISRM, user participation in capacity building interventions is expected to also have a positive effect on an organization's security.

Proposition 1: User participation in information security capacity building interventions within CBOs positively contributes to knowledge transfer from the source to the recipient of the intervention.

Motivation

A person's motivation to take part in a training intervention has been found to influence the extent to which knowledge is transferred during the intervention (Ko et al., 2005). In the present study, CBO staff members' motivation to participate in a capacity building intervention is examined, including *why* they are motivated. Therefore, self-determination theory (SDT; Ryan & Deci, 2000; Gagne &Deci, 2000) is used as a lens for examining the type of motivation one may have to participate in an ISRM intervention. According to SDT, motivation may be autonomous (i.e., one performs an activity of his/her own volition) or controlled (i.e., one performs an activity due to pressure, including the potential for reward or punishment). SDT defines a taxonomy of motivation types on a continuum from controlled (i.e., extrinsic) to autonomous (i.e., intrinsic) motivation, as described in Table 1 (Ryan & Deci, 2000; Gagne &Deci, 2000).

According to Chen (2014), the nonprofit literature emphasizes intrinsic motivation, resulting in limited research on extrinsic motivation of nonprofit managers. Given that managing informa-

Table 1. Motivation in self-determination theory

Motivation Type	Definition
External	Also referred to as extrinsic motivation and is based on perceived reward or punishment of the behavior.
Introjected	People perform such actions with the feeling of pressure in order to avoid guilt or anxiety or to attain ego-enhancements or pride.
Identified	The activity is congruent with the person's values; the person identifies with the importance of a behavior and has thus accepted its regulation as his or her own.
Integrated	The behavior is an integral part of who the person is, and is thus self-determined.
Intrinsic	The doing of an activity for its inherent satisfactions rather than for some separable consequence.

tion security is required by external entities (e.g., regulatory and funding agencies), motivation to improve security is inherently externally driven to some degree.

SDT posits that extrinsic motivation may be internalized to varying degrees. That is, internalization of external regulation is conceptualized in SDT as an overarching term that comprises introjection, identification, and integration, with integration being the most autonomous (Gagne & Deci, 2005).

Proposition 2: Motivation positively contributes to the extent to which users will participate in an information security capacity building intervention.

Absorptive Capacity

From a cognitive perspective, absorptive capacity refers to "the set of organizational routines and processes by which organizations acquire, assimilate, transform, and exploit knowledge to produce dynamic organizational capabilities" (Malhotra et al., 2005). Absorptive capacity is largely a function of the participant's existing knowledge prior to the intervention and is believed to be positively related to knowledge transfer (Ko et al., 2005; San Nicolas-Rocca et al., 2014; Puhakainen & Siponen, 2010). That is, to the extent that participants have had experience or have existing knowledge in some related area, knowledge transfer is more likely to take place between the external collaborator administering the intervention and the organizational members receiving the intervention within CBOs.

It is noteworthy that knowledge related to a capacity building intervention in information security is not limited to information security. For example, a participant who has knowledge of relevant organizational processes being assessed (e.g., user provisioning for an ERP system); end user computing use within the organization (e.g., mobile device use); or organizational policies (e.g., employee remote access policy) is expected to have the absorptive capacity needed to successfully engage in knowledge transfer within a capacity building intervention in information security. Similarly, previous experience with or prior knowledge of risk assessment, audit, or other capacity building initiatives is expected to facilitate knowledge transfer in the present context. Thus, a participant's relevant previous experience and knowledge can aid knowledge transfer during information security capacity building.

Proposition 3: Absorptive capacity positively influences knowledge transfer from the source to the recipient of a capacity building intervention within a CBO.

Communication

A training program depends on the ability of the training facilitator to engage trainees (Cone et al., 2007). When the facilitator is able to effectively communicate the applicability and practical purpose of the material to be mastered, as distinguished from abstract or conceptual learning, the learning retention rates and the subsequent transference of the new knowledge or skill to the trainees is enhanced (NIST SP 800-16, 1998). Thus, another important factor in a training (i.e., capacity building) intervention's ability to result in knowledge transfer is communication. Extant research on knowledge sharing, transfer and integration has examined communication in multiple ways. Examples include the type of communication between team members (Teo & Bhattacherjee, 2014); the competence of the source (e.g., trainer) to communicate effectively and the competence of the recipient to listen effectively (Ko et al., 2005); the amount of communication flow between the source and recipient (Minbaeva et al., 2014); the perceived quality of the

communication among people (Rodriguez & Edwards, 2014); and the extent to which training focuses on what the recipients need to know as opposed to unrelatable broadcast of "technocratic" facts (Stewart & Lacey, 2012). These studies have collectively found that knowledge transfer can only occur if communication is effective in terms of type, amount, competence, and usefulness.

Proposition 4: Effective communication positively contributes to knowledge transfer from the source to the recipient in a capacity building intervention within a CBO.

Knowledge Utilization

Knowledge transfer is particularly useful when conceptualized through the lens of knowledge utilization; that is, examining how knowledge is used as a result of its transfer (Teo & Bhattacherjee, 2014). In a capacity building intervention on information security, what is of particular interest is the extent to which a CBO uses the knowledge transferred to actually strengthen its information security practices. In the present study, knowledge utilization is demonstrated when the CBO subsequently takes action in ISRM as a result of the capacity building intervention.

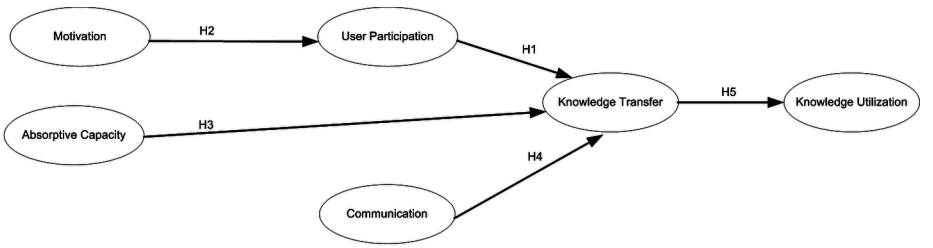
ISRM is the process of identifying and prioritizing IS security risk, and implementing and monitoring security safeguards (i.e., countermeasures; controls) that address those risks (Spears & Barki, 2010). ISRM is concerned with protecting information assets from compromise in high-risk scenarios, while balancing the cost of safeguards against the level of security provided and the accessibility of information resources to end-users (Shedden et al., 2010). Examples of activities performed as part of ISRM include designing, implementing, and evaluating policies, procedures, or technologies to conduct risk assessments; managing access control; managing BYOD (bring your own device) risk; etc. Knowledge transferred on these topics is expected to result in action taken to manage risks and solutions addressed during the intervention.

Proposition 5: Knowledge transfer from an information security capacity building intervention positively contributes to knowledge utilization in managing security risk within a CBO.

THEORETICAL MODEL

According to the theoretical model presented in Figure 1, knowledge transfer is influenced by a CBO member's motivation to participate and his/her absorptive capacity (i.e., capacity to absorb the information presented during the intervention) prior to the start of the intervention. The degree of user participation and the communication that takes place during the intervention also influence knowledge transfer. To the extent that knowledge transfer takes place, CBO participants

Figure 1. The effect of knowledge transfer in an information security capacity building intervention



are expected to use the knowledge gained by taking action that strengthens information security within the organization. Action may include implementing new or revised security policies, procedures or technologies to improve security.

EXPLORATORY STUDY

The model in Figure 1 is examined as part of an exploratory study within the context of a service learning course on information security risk assessment. The study is considered exploratory, because there was no a priori theory used during data collection. Instead, the theoretical model in Figure 1 was subsequently developed as a lens through which to examine the qualitative data. Following the exploratory study, the model will be examined using a larger pool of nonprofit organizations. A university's 'center for community-based service learning' has over 300 active partnerships with CBOs and has partnered with the research team to identify CBOs for the course and the subsequent larger research study. This section presents initial findings from the exploratory study.

Data Collection

During the exploratory study, the work performed during the service learning course is the capacity building intervention. The course is offered once annually with average enrollment of 15-20 students. CBO partners are recruited for the course by answering a Call for Partners (CFP) questionnaire distributed by the University's center for community-based service learning. The CFP describes the course objectives and informs respondents that students do not need access to client information in order to conduct the assessment. The CFP then asks the respondents at prospective CBOs to indicate whether sensitive client information is stored; to check boxes in a list of security categories that may be of particular concern (e.g., access control, bring your own device, etc.), and to briefly describe any area they want students to work on in relation to assessing security needs. Finally, the CFP asks the number of total employees at the prospective CBO; the number of IT staff; whether the CBO is connected to a network; whether the CBO has a security policy, and whether the CBO has had a risk assessment within the past 3 years.

Prospective CBOs are those that provide health or human services that require them to maintain sensitive client data; such organizations are targeted due to 'need' from a data sensitivity perspective. Given student enrollment and team sizes of 3-4 students per course offering, 4-5 CBO partners are selected per course. In the two years the course has been offered, more CBOs requested participation than slots available. Thus, CBO recruitment is feasible.

Eight CBOs have participated in the course. The primary contact (PC) person at the CBO who is working with the research team is typically the person who completed the CFP. As shown in Table 2, PCs have included an executive director, a quality assurance (QA) manager, business managers, and IT staff. The number of internal employees has ranged from 5 to 200, though the majority of participating CBOs have over 50 paid employees. CBOs have an average of one internal IT staff person. The majority of CBOs have a security policy. However, most have not done a risk assessment in the last three years. Participating CBOs typically have annual revenues of $1 to $10 million. Some CBOs have a single site, while others have multiple facilities.

Prior to the start of the course, the research team visited each participating CBO's site and met with at least the PC. The purpose of the meeting was twofold: first, to introduce the course, the process, and the schedule to the PC and any other designated staff. The second purpose of the pre-intervention meeting was for the researchers to gain a contextually informed understanding

Table 2. Participating CBOs

CBO Services	PC	Paid Staff	IT Staff	Sec Policy	Risk Assessment in 3 Yrs
Foster care home & school	Exec Dir	125	1	Y	N
Behavioral health counseling & substance abuse treatment	QA	120	1	Y	N
Prison release work transition programs	Mgr	25	0	N	N
Mortgage counseling	Mgr	25	0	Y	N
Community development	Mgr	5	0	N	N
Family services; daycare	IT	130	1	Y	Y
Early childhood education; svcs for adults w/disabilities	Mgr	150	1	Y	N
Adult education; substance abuse counseling	IT	180	3	Y	N

of the CBOs over-arching security needs for the course (i.e., the ISRM intervention). Once the course began, student teams met with an average of 3 to 5 staff members per CBO.

Students conducted a risk assessment at the CBO by interviewing participants on-site, conducting facility walkthroughs to observe security strengths and weaknesses, and policy review. Students use a risk questionnaire developed by the research team as a guide on what to assess and discuss with user participants; they could also ask additional questions. Using the National Institute of Standards and Technology's "Guide for Conducting Risk Assessments" (NIST SP 800-30) as a framework, students analyzed data collected and then wrote a detailed (e.g., 25-30 pages) risk assessment report. Consistent with other capacity building research projects (e.g., Kindred & Petrescu, 2015), the present capacity building intervention was tailored to each CBO in that there was a needs assessment, followed by tailored recommendations to address identified risks. In total, approximately six in-person meetings and two written results were provided during an eleven-week intervention.

Data Analysis

Using the theoretical model presented in Figure 1 as a framework of analysis, initial findings from the first two years of the exploratory study are discussed next.

Motivation

A variety of motivations were cited for PCs initiating participation in the ISRM intervention. One organization was in the early stages of implementing a new project that would involve very sensitive data shared with external psychiatrists who were not part of the state-controlled secured network. The PC (an executive director) wanted students to assess the risk in cloud storage and data transmission processes. Two other PCs (a quality assurance manager and an IT manager) at different CBOs cited upcoming state program audits as partial motivation. The ISRM intervention was seen as an opportunity to improve security prior to state audits containing a relatively small portion on information handling. A fourth PC indicated he was hoping the ISRM intervention

would help raise security awareness among end users whom he had observed having poor security practices. He also wanted to raise security awareness among business management, and he was open to gaining additional knowledge on any newly discovered security risks the student teams might uncover. The remaining PCs generally expressed as motivation their awareness of the sensitivity of client information maintained by their organizations, and the need to improve internal security practices and policies.

Absorptive Capacity

Most PCs had some type of relevant prior experience. For example, the executive director had prior experience with implementing policy and allocating resources in his organization. He had worked with the IT staff person on setting up a cloud solution for securely storing client information. He was versed in a secure email communication system run by the state government. Another PC was a QA manager who had significant experience with internal audits. Though she had limited experience with information security projects, she was aware enough to request help with incidence response and bring your own (mobile) device (BYOD) risks. The PCs who were IT staff persons had some experience with implementing network security safeguards. The PC at the smallest participating CBO, a business development manager, had recently set up a computer backup process for his organization. Two of the PCs appeared to have no prior experience with information security policy-making and very limited technical background. In both cases, these CBOs did not have IT staff.

As shown in Table 1, six of 8 participating CBOs had security policies. Only one CBO had a risk assessment within the 3 years prior to the ISRM intervention in this study. This same CBO also purportedly had multiple security-related policies, yet the PC could not locate them for the student team's review, suggesting the policies were not actively used or monitored. Prior to the study, another CBO also had multiple security-related policies that appeared to be boilerplate; it was not apparent the policies had been communicated or used in the organization.

User Participation

The study found that user participation is an important element of an ISRM intervention within a CBO. For 6 of the 8 participating CBOs, the project coordinator was a non-IT employee (i.e., end user). As the PC, these users participated in the ISRM intervention by being interviewed by student teams, arranging for students to meet with relevant roles within the CBO for additional interviews, providing documentation, and visiting campus for the project launch and again to hear student teams' final presentations. PCs also acted as subject matter experts on information usage, end user technology usage, policies, and processes within their organizations.

In contrast, for the two CBOs that had IT staff as PCs, a lack of user participation was problematic. That is, IT staff performing the role of PC in the ISRM intervention were unable to get management to meet with student teams. While the IT staff person was interested in a security intervention, business management did not answer calls for meeting with the instructor or the student teams. Thus, those who would have to improve any policy, procedural, or funding changes in security chose not to participate, rendering highly unlikely any significant knowledge transfer on security across the organization.

In summary, user participation was integral to gaining buy-in (Spears & Barki, 2010) on the ISRM intervention and access to decision-makers within the organization.

Communication

The university and CBO collaborators communicated approximately 6 times during each security intervention. First, the instructor met with the PC at the CBO's site prior to the start of the course to explain the security assessment process, course objectives, and to gain an understanding of the CBO's context and high-level security needs. Second, during the first night of class, the PC attended class in order to meet students, introduce their organizations to students, and begin initial discussions on planning for the security assessment intervention. Third, student teams met at the CBO site at least once, sometimes twice, in order to interview staff, walkthrough the facility to observe security practices, and gain access to relevant organizational policies and documents. From this on-site assessment, students wrote a detailed risk assessment report.

The security risk assessment report was presented by the student team to the PC (and other staff the PC may have invited) either in person, via conference call, or by email, depending on CBO participant availability. The report contained a description of the risk assessment process performed, a table and explanations of security vulnerabilities found by the student team, ranked by severity, and a list of low-cost recommendations to correct security weaknesses. Given the limited time of an academic quarter, student teams could only feasibly provide more detailed guidance on a smaller set (e.g., 3) of security recommendations. Therefore, CBO representatives had an opportunity to indicate on which security recommendations they preferred students to provide more detailed guidance. If no preference was provided, then students chose a set of approximately 3 security safeguards to provide more detailed guidance that included a design and test plan per safeguard. This information was appended to the initial risk assessment report and was presented to the PC (and possibly additional invitees of the PC) on-campus during the last night the class meets.

In summary, communication occured via face-to-face interaction, a written report, and safeguard designs written as tutorials. Although the exploratory study was able to assess the type and amount of communication, it was difficult to assess effectiveness. That is, the PCs enjoyed working with the student teams and only made positive comments, possibly unwilling to complain about any potential perceptions of student team communication ineffectiveness.

Knowledge Transfer

In an information security risk assessment intervention, knowledge transfer needs to occur at two levels in order to accomplish the goal of improved security practices. First, security knowledge from the trainer (the source) must be transferred to the trainee (the recipient). Second, the trainee (e.g., the PC and other CBO staff who participated in the intervention) must transfer security knowledge to decision-makers and/or other CBO staff so that improvements are possible. Thus, the research team encouraged PC's to include upper management in some aspect of the intervention, either meeting student teams on-site, attending final presentations, or presenting student findings in internal meetings. Six of the eight PCs were able to engage higher-level management; the two IT staff member PCs were not.

In addition to *who*, the concept of knowledge transfer also concerns *what* knowledge to transfer. An emphasis was placed on communicating in laymen's (i.e., non-techie) terms security risks found within the CBOs operational environment. Furthermore, security recommendations were typically either procedural or available features in existing software (i.e., incurred no direct costs). Where new security software was recommended, free-to-low cost solutions were sought. In some cases, policies were designed.

On average, 15-20 security risks were identified per CBO. For example, student teams found instances of volunteers using staff network login credentials; file cabinet keys in plain view in high-traffic visitor areas; lack of encrypted storage; sensitive information displayed on computer monitors when worker was away from workstation; weak access control on shared network drives; etc. In addition to communicating these risks, knowledge transfer also included BYOD policy; incidence response policy; tutorial on creating new user accounts in Windows; tutorial on auto-lock screensavers; email configuration to manage remote mobile device connections; tutorial on VPN setup; comparison of security features among cloud storage solutions; general security training slides; etc.

Knowledge Utilization

There was evidence of knowledge utilization. On the one hand, there was evidence of CBOs implementing 'quick fixes' such as securing file cabinet keys; moving important paper records from under a ceiling sprinkler; locking the file server in a room; moving sensitive papers insecurely stored in boxes in plain view to a locked room, etc. On the other hand, even though student teams emphasized low-cost, relatively simple to implement solutions, labor was still an issue with implementing some recommended security safeguards. For example, one PC liked the security training materials provided by a student team, but admitted to not having the internal staff to implement it. However, two other CBOs each created a new IT position in direct response to the student teams' recommendations. Finally, in some cases, PCs indicated their organization planned to implement some of the recommended security procedures, such as assigning volunteers unique network login IDs. However, future research is needed to determine the extent to which these solutions were implemented. That is, did security policies and practices later become institutionalized?

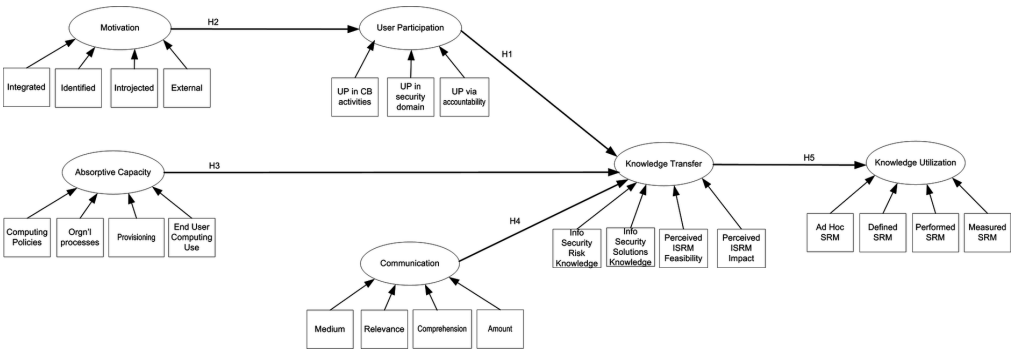
MEASURES FOR COMFIRMATORY STUDY

Informed by the exploratory study and the literature, this section describes how each theoretical construct in Figure 1 will be measured in a future confirmatory study. With the exception of user participation, the authors are unaware of existing measurement scales in an information security context for the remaining model constructs. Therefore, measurement scales are developed for the knowledge transfer, knowledge utilization, motivation, absorptive capacity. Figure 2 shows the indicators for each construct. Survey items are provided in the Appendix.

Knowledge Transfer

Consistent with previous research that has measured knowledge transfer (Ko et al., 2005; Teo & Bhattacherjee, 2014), knowledge transfer is measured as the extent to which a CBO participant acquired knowledge or understands some key training objective. In particular, four formative indicators measure the extent to which the participant has acquired knowledge on the security risks identified within the organization; acquired knowledge on solutions to manage identified risks; gained an understanding of the feasibility to implement security solutions; and gained an understanding of the potential impact if security solutions are not implemented to manage identified risks.

Figure 2. Theoretical model with indicators



Knowledge Utilization

Conceptually, the desired outcome of knowledge transfer is knowledge utilization (Teo & Bhattacherjee, 2014; Jennex & Durcikova, 2014). In the present study, ISRM capability maturity is an indicator of knowledge utilization; i.e., action was taken within the organization following knowledge transfer. In conceptualizing ISRM capability maturity as knowledge utilization, the extent to which CBOs are actually 'doing' ISRM is examined. Four formative indicators are used to measure the extent to which CBO participants have implemented ad hoc security safeguards; documented new or revised security safeguards; performed security safeguards according to their documented definition; or evaluated security safeguard performance. These four indicators use a Likert scale and represent Levels 1-4 of the capability maturity model. (See Spears et al., 2013 for an overview of capability maturity in information security.) In short, capability maturity measures whether security policies and procedures were merely implemented on an ad hoc (e.g., perhaps one-time) basis, or whether they were actually formally adopted and monitored (i.e., institutionalized). A higher degree of capability maturity is preferred, as this would indicate the knowledge transferred resulted in on-going security safeguard performance.

User Participation

In adapting Spears and Barki's (2010) conceptualization of user participation in IS security to the present study, users may participate in an information security capacity building intervention by performing specific activities, focusing on particular areas of security (e.g., access control; BYOD; etc.), or being accountable or responsible for some aspect of data protection. Thus, user participation (UP) is measured as three formative indicators: UP in capacity building activities; UP in security domains; and UP via accountability. Each of these three measures is a separate index of 7 items (see the Appendix for a list of survey items). The more items checked, the higher a participant's score for a given measure.

Motivation

In answering a call for researchers to pay attention to extrinsic motivation in nonprofit management research (Chen, 2014), SDT (Ryan & Deci, 2000; Gagne &Deci, 2000) is applied as a framework for measuring motivation. Extrinsic motivation is examined given that ISRM is required and/or expected by external entities, such as regulatory and funding agencies, and

clients. Given that extrinsic motivation is not unidimensional (Chen, 2014), and instead may be internalized to various degrees (Gagne & Deci, 2005), motivation is measured as four formative indicators: integrated, identified, introspection, and external. These indicators vary, respectively, in a continuum of more to less autonomy (self-determination) in why participants are motivated to be part of an information security capacity building intervention.

Absorptive Capacity

The proposed capacity building intervention is focused on how to manage risk of a particular type (i.e., information security). Thus, existing knowledge on internal computing-related policy (e.g., acceptable use policy) is expected to contribute to knowledge transfer in the present study. Secondly, existing knowledge on organizational (business) processes relevant to an IS security risk assessment (e.g., client intake) have been found to contribute to positive outcomes in information security (Spears & Barki, 2010), and thus is an indicator of absorptive capacity. Finally, participant knowledge (e.g., from observation) of computing use by organizational members is expected to contribute to participants' ability to absorb materials on end-user related security risk presented during a capacity building intervention. Thus, absorptive capacity will be measured as four formative indicators: existing knowledge of the organization's computing-related policies; relevant organizational processes; provisioning; and end user computing use.

Communication

Four formative indicators are used to measure communication effectiveness, based on the literature (Cone et al., 2007; NIST SP 800-16, 1998; Teo & Bhattacherjee, 2014; Minbaeva et al., 2014; Stewart & Lacey, 2012). Training material effectiveness; the relevance of the training to the participant; the participant's comprehension of the trainer's oral communication; and the amount of communication contribute to its effectiveness.

RESEARCH IMPLICATIONS

A theoretical model on knowledge transfer in information security risk management was presented and then used as a framework of analysis for an exploratory study on security risk assessment interventions within eight CBOs. The goal of the security intervention was to enable participating CBOs to make improvements in information security within their organizations. Knowledge transfer was examined as a means to reach this goal. When knowledge is transferred from the trainer to the trainee, knowledge utilization becomes possible. Indeed, the present study found evidence of security improvements in five of the eight participating CBOs, with another CBO representative indicating he would work with his IT service provider to implement some of the recommendations. Future research is needed to determine whether these improvements were institutionalized, as opposed to one-time ad hoc measures.

Within the eight participating CBOs, internal IT staff ranged from zero to three in each CBO, with an average of one internal IT staff member. While effective information security intuitively requires all organizational members' participation, end user knowledge of how to manage security risk is particularly important when an organization has little-to-no internal IT staff. The study also found that having end users as the primary contact was instrumental in getting organizational decision-makers to participate in the assessment. In contrast, when IT staff members were the primary contact, decision-makers did not answer requests to participate in the assessment. Thus,

if the goal is to include end users (e.g., as subject matter experts) in a security risk assessment, having user participation in a leadership or coordinator role is essential.

A practical implication of this work relates to its longer-term aim to help CBOs strengthen their information security. Furthermore, studying CBOs contributes to filling a gap in knowledge on security practices and weaknesses within CBOs – an important research topic given the sensitivity of data maintained by CBOs.

Finally, university engaged scholarship (Schensul, 2010) can provide a "win-win" to both CBOs in need of information security capacity building and academic researchers in need of realistic contexts. Thus, an implication of this work is the promotion of university-engaged scholarship that can benefit under-resourced CBOs that typically serve under-represented communities.

PLAN FOR FUTURE RESEARCH

Our plan for future research is to first assess content validity of the survey items shown in the Appendix. Next, a confirmatory study will be conducted to quantitatively test the theoretical model presented in Figure 2. Data will be collected online from a larger number of organizations. In place of face-to-face interventions performed during the exploratory study that was part of a service learning course, data will be collected online for the confirmatory study using a self-assessment questionnaire.

As part of the exploratory study, the research team has developed R-Score, a security risk self-assessment questionnaire. R-Score contains approximately 50 questions on internal security practices, organized by 8 topic domains. Security questions are practical and designed so that end users can reasonably answer the security risk questionnaire. One to many respondents from a single organization may respond to R-Score; the more respondents the better for a more representative score. All responses are used to compute a risk score within the scope of the tool that is analogous to a report card, based on answers for each of the 8 topic domains included in the questionnaire. R-Score will also provide basic security training materials based on industry standards. The self-assessment tool will be available online. Prospective participants must agree to answer pre- and post-study surveys in exchange for access to the self-assessment tool. The pre- and post-study surveys will collectively test the full theoretical model in Figure 2.

CONCLUSION

CBOs in the health and human services sector handle very sensitive information. However, many of these CBOs lack the resources needed to identify and manage information security risks within their environment. This paper highlighted the need for information security risk management interventions within CBOs and proposed a theoretical model that was used to examine how interventions provided by university collaborators may result in strengthened information security.

ACKNOWLEDGMENT

The authors would like to thank the co-chairs and participants of the Knowledge Systems Track at the 49th Hawaiian International Conference on System Sciences (HICSS) for their valuable comments on the preliminary findings presented at the conference.

REFERENCES

Berman, H. (2010). Meeting Community Needs. *Inquiry*, *47*(3), 186–198. doi:10.5034/inquiryjrnl_47.03.186 PMID:21155414

Chen, C. (2014). Nonprofit Managers' Motivational Styles: A View Beyond the Intrinsic-Extrinsic Dichotomy. *Nonprofit and Voluntary Sector Quarterly*, *43*(4), 737–758. doi:10.1177/0899764013480565

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A Video Game for Cyber Security Training and Awareness. *Computers & Security*, *26*(1), 63–72. doi:10.1016/j.cose.2006.10.005

Gagne, M., & Deci, E. L. (2005). Self-Determination Theory and Work Motivation. *Journal of Organizational Behavior*, *26*(4), 331–362. doi:10.1002/job.322

Imboden, T. R., Phillips, J. N., Seib, J. D., & Fiorentino, S. R. (2013). How are Nonprofit Organizations Influenced to Create and Adopt Information Security Policies? *Issues in Information Systems*, *14*(2), 166–173.

Jennex, M., & Durcikova, A. (2014). Integrating IS Security with Knowledge Management: Are We Doing Enough? *International Journal of Knowledge Management*, *10*(2), 1–12. doi:10.4018/ijkm.2014040101

Kindred, J., & Petrescu, C. (2015). Expectations Versus Reality in a University Community Partnership: A Case Study. *Voluntas*, *26*(3), 823–845. doi:10.1007/s11266-014-9471-0

Ko, K., Kirsch, L., & King, W. (2005). Antecedents of Knowledge Transfer from Consultants to Clients in Enterprise System Implementations. *Management Information Systems Quarterly*, *29*(1), 59–85.

Malhotra, A. Gosain, S. & El Sawy, O.A. (2005). Absorptive Capacity Configurations in Supply Chains: Gearing for Partner-Enabled Market Knowledge Creation, *MIS Quarterly* (Special Issue on Information Technologies and Knowledge Management), 29(1), 145-187.

Minbaeva, D., Pedersen, T., Bjorkman, I., Fey, C. F., & Park, H. J. (2014). MNC Knowledge Transfer, Subsidiary Absorptive Capacity and HRM. *Journal of International Business Studies*, *45*(1), 38–51. doi:10.1057/jibs.2013.43

Minzner, A., Klerman, J. A., Markovitz, C. E., & Fink, B. (2014). The Impact of Capacity-Building Programs on Nonprofits: A Random Assignment Evaluation. *Nonprofit and Voluntary Sector Quarterly*, *43*(3), 547–569. doi:10.1177/0899764013491013

National Institute of Standards and Technology (NIST). (1998). Information Technology Training Requirements: A Role- and Performance-Based Model (NIST Special Publication 800-16). Washington DC: US Department of Commerce.

Pennsylvania eHealth Partnership Authority. (n. d.). Fact Sheet: Super-Protected Data. Retrieve from http://www.paehealth.org/images/Super_Protected_Data_Fact_Sheet_FINAL_20150313.pdf

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance through Information Systems Security Training: An Action Research Study. *Management Information Systems Quarterly*, *34*(4), 767–A4.

Rodriguez, E., & Edwards, J. S. (2014). Knowledge management in Support of Enterprise Risk Management. *International Journal of Knowledge Management*, *10*(2), 44–62. doi:10.4018/ijkm.2014040104

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary Educational Psychology*, *25*(1), 54–67. doi:10.1006/ceps.1999.1020 PMID:10620381

San Nicolas-Rocca, T., Schooley, B., & Spears, J. L. (2014). Designing Effective Knowledge Transfer Practices to Improve IS Security Awareness and Compliance. *Proceedings of the 47th Annual Hawaii International Conference on System Sciences*, (pp. 3432-3441). Computer Society Press.

San Nicolas-Rocca, T., Schooley, B., & Spears, J. L. (2014). Exploring the Effect of Knowledge Transfer Practices on User Compliance to IS Security Practices. *International Journal of Knowledge Management*, *10*(2), 62–78. doi:10.4018/ijkm.2014040105

Schensul, J. J. (2010). Engaged Universities, Community Based Research Organizations and Third Sector Science in a Global System. *Human Organization*, *69*(4), 307–320. doi:10.17730/humo.69.4.2g40869150316302

Shedden, P., Ruighaver, A. B., & Ahmad, A. (2010). Risk Management Standards - the Perception of Ease of Use. *Journal of Information Systems Security*, *6*(3), 23–41.

Sobeck, J. L. (2008). How Cost-Effective Is Capacity Building in Grassroots Organizations? *Administration in Social Work*, *32*(2), 49–68. doi:10.1300/J147v32n02_04

Spears, J., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *Management Information Systems Quarterly*, *34*(3), 503–522.

Spears, J. L., Barki, H., & Barton, R. R. (2013a). Theorizing the Concept and Role of Assurance in IS Security. *Information & Management*, *50*(7), 598–605. doi:10.1016/j.im.2013.08.004

Stewart, G., & Lacey, D. (2012). Death by a Thousand Facts: Criticizing the Technocratic Approach to Information Security Awareness. *Information Management & Computer Security*, *20*(1), 29–38. doi:10.1108/09685221211219182

Teo, T. S. H., & Bhattacherjee, A. (2014). Knowledge Transfer and Utilization in IT Outsourcing Partnerships: A Preliminary Model of Antecedents and Outcomes. *Information & Management*, *51*(2), 177–186. doi:10.1016/j.im.2013.12.001

Wetta-Hall, R., Ablah, E., Oler-Manske, J., Berry, M., & Molgaard, C. (2004). Strategies for Community-Based Organization Capacity Building Planning on a Shoestring Budget. *The Health Care Manager*, *23*(4), 302–309. doi:10.1097/00126450-200410000-00003 PMID:15638337

Janine L. Spears is an Assistant Professor at DePaul University's School of Computing where she teaches courses in information security management and legal issues in information assurance. Her research focuses on information security risk assessment and user participation. Dr. Spears' research has been published in MIS Quarterly*, the* International Journal of Knowledge Management, Information & Management*, and the* Journal of Information Systems Education*. She holds a PhD from the Smeal College of Business at Penn State University.*

Tonia San Nicolas-Rocca is an Assistant Professor in the School of Information at San Jose State University. She holds a PhD in Information Systems and Technology from Claremont Graduate University. Her research interests include cybersecurity, health informatics, and knowledge management. Dr. San Nicolas-Rocca has published her work in numerous peer-reviewed research journals and conference proceedings.

APPENDIX

Knowledge utilization, knowledge transfer, motivation, and communication use a Likert scale. The measurement scale for user participation is in the form of an index, where an individual's score is the number of checks per UP item. Absorptive capacity is measured on a scale of: none, minimal, somewhat, significant, very, expert (see Table 3).

Table 3. Survey items per construct

Indicator	Survey Item per Construct
Knowledge Utilization	
	Question: Since the completion of the training intervention, I have ___:
Ad hoc SRM	*Performed* additional security procedures within the organization on an ad hoc, informal basis.
Defined SRM	*Worked* on *defining* new or revised security policies.
Performed SRM	*Implemented* new or revised security procedures for organizational staff to follow.
Measured SRM	*Evaluated* at least one security safeguard to determine whether it is being followed by organizational staff.
Knowledge Transfer	
	Question: During this capacity building intervention, ____:
Info Security Risk Knowledge	I acquired knowledge on information security risks within my organization.
Info Security Solutions Knowledge	I acquired knowledge on solutions to manage information security risks identified within my organization.
Perceived ISRM Feasibility	I gained an understanding of the feasibility to implement solutions to manage information security risks identified within my organization.
Perceived ISRM Impact	I gained an understanding of the potential impact of <u>not</u> implementing solutions to manage information security risks identified within my organization.
User Participation (UP)	
	Question: As part of the information security capacity building intervention:
UP in Capacity Building Activities	Did you perform any of the following activities? (Check all that apply) • Security questionnaire • Interview with external collaborator (i.e., trainers) • Facility tour/walkthrough with external collaborator • Policy review • Business or IT process workflow analysis • Communication with internal peers or staff on training materials • Communicate with internal senior management on training materials
UP in Security Domains	Did you participate in discussions on the following areas of security? (Check all that apply) • Password policy • User provisioning (i.e., establishing or revoking user logons and system authorization) • Mobile device • Encryption • Vendor security • Physical security • Disaster recover, business continuity, or security incident response
UP via Accountability	Were you formally responsible or accountable in the following ways? (Check all that apply) • Identifying organizational members to participate in training • Communicating results to upper management • Communicating results to peers or staff • Responsible for organizational compliance of funder requirements • Responsible for organizational compliance with government regulations • Responsible for internal audit • Responsible for communicating organizational risk to the Board of Directors

continued on following page

Table 3. Continued

Indicator	Survey Item per Construct
Motivation	
	Question: I am motivated to participate in this security training because:
Integrated	I wholeheartedly feel responsible to protect our clients from harm.
Identified	I believe it is important to protect our clients' sensitive data.
Introjected	I would be embarrassed if my organization experienced a data breach.
External	My job could be in jeopardy if my organization were to experience a data breach.
Absorptive Capacity	
	Question: How would you rate your knowledge:
Computing policies	Of your organization's computing-related policies for internal staff computer usage?
Orgn'l processes	Of your organization's work processes that handle sensitive client information?
IS provisioning	How access to client information is granted?
End user computing	How internal staff tend to use computing devices to access organizational information?
Communication	
Medium	The training materials used communicated security lessons effectively.
Relevance	Communication during the training was effective in focusing on things I needed to know about security for my job.
Comprehension	The trainer's oral communication with me was understandable.
Amount	The amount of time communicating about security was sufficient for me to learn.