Information Security in Libraries: Examining the Effects of Knowledge Transfer

Tonia San Nicolas-Rocca
and Richard J. Burkhard

ABSTRACT

Libraries in the United States handle sensitive patron information, including personally identifiable information and circulation records. With libraries providing services to millions of patrons across the U.S., it is important that they understand the importance of patron privacy and how to protect it. This study investigates how knowledge transferred within an online cybersecurity education affects library employee information security practices. The results of this study suggest that knowledge transfer does have a positive effect on library employee information security and risk management practices.

INTRODUCTION

Libraries across the U.S. provide a wide range of services and resources to society. Libraries of all types are viewed as important parts of their communities, offering a place for research, to learn about technology, to access accurate and unbiased information, and a place that inspires and sparks creativity. As a result, there were over 171 million registered public library users in the U.S. in 2016.[1]

A library is a collection of information resources and services made available to the community in which it serves. The American Library Association (ALA) affirms the ethical imperative to provide unrestricted access to information and to guard against impediments to open inquiry.[2] Further, in all areas of librarianship, best practice leaves the library user in control of as many choices as possible.[3] In a library, the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others.[4]

Many library resources require the use of a library card. To obtain a library card in the U.S. one must provide official photo identification showing personally identifiable information (PII), such as name, address, telephone number, and email address. PII connects library users or patrons with, for example, items checked out, and websites visited. As such, PII has the potential to build up an image of a library patron that could potentially be used to assess the patron's character. In response, the ALA developed a policy concerning the confidentiality of PII about library users.[5] Confidentiality extends to "information sought or received and resources consulted, borrowed, acquired or transmitted," and includes, but is not limited to, database search records, reference interviews, circulation records, interlibrary loan records, and other personally identifiable uses of library materials, facilities, or services.[6] In more recent years, the ALA has further specified that the right of patrons to privacy applies to any information that can link "choices of taste, interest, or research with an individual."[7] When library users recognize or fear that their privacy or

Tonia San Nicolas-Rocca (tonia.sannicolas-rocca@sjsu.edu) is Assistant Professor in the School of Information at San Jose State University. **Richard J. Burkhard** (richard.burkhard@sjsu.edu) is Professor in the School of Information Systems and Technology in the College of Business at San Jose State University.

confidentiality is compromised, true freedom of inquiry no longer exists. Therefore, it is imperative that libraries use extra care when handling patron personally identifiable information.

While librarians and other library employees may understand the importance of data protection, they generally don't have the resources available to assess information security risk, employ risk mitigation strategies, or offer security education, training, or awareness (SETA) programs. This is of particular concern as libraries increasingly have access to databases of both proprietary and personal information.[8] SETA programs are risk mitigation strategies employed by organizations worldwide to increase and maintain end-user compliance of information security and privacy policies. In libraries, information systems are widely used to provide services to patrons, however, there is little known about information security practices in libraries.[9] Given the sensitivity of the data libraries handle, and the lack of information security resources available to them, it is important for those currently or planning to work in the library environment to develop the knowledge necessary to identify risks and develop and employ risk mitigation strategies to protect information and information resources they are entrusted with. Therefore, the research question in this present study is: *How can cybersecurity education strengthen information security practices in libraries?*

Currently, there is a dearth of research on information security practices in libraries.[10] This is an important research gap to acknowledge given that patron privacy is fundamental to the practice of librarianship in the U.S, and the advancement in technology coupled with federal regulations adds to the challenges of keeping patron privacy safe.[11] Thus this study contributes to current literature by evaluating the effects of knowledge transfer as a means to strengthen information security within libraries. Furthermore, this study will offer a preliminary investigation as to whether knowledge utilization leads to motivation and the participation of information security risk management activities within libraries.

The remainder of this paper proceeds as follows: First, a review of knowledge transfer is covered. A description of the cybersecurity course, including students and course material, is provided. Data collection and analysis are then presented. This is followed by a discussion of the findings, limitations, and future research.

LITERATURE RIVEW

Knowledge Transfer in SETA

Knowledge transfer through SETA programs plays a key role in the development and implementation of cybersecurity practices.[12] Knowledge is transferred when learning takes place and when the recipient of that knowledge understands the intricacies and implications associated with that knowledge so that he or she can apply it.[13] For example, in a security education program, an educator may transfer knowledge about information security risks to users who learn and apply the knowledge to increase patron privacy. The knowledge is applied when evidenced by users who are able to identify risks to patron data and implement risk mitigations strategies that serve to protect patron information and information system assets.

Knowledge transfer can be influenced by four factors: absorptive capacity, communication, motivation, and user participation.[14] This study evaluates the extent to which knowledge transferred from a cybersecurity course strengthens information security practices within libraries. This study adapts the theoretical model as proposed by Spears & San Nicolas-Rocca

(2015) (see figure 1) to examine the effects of cybersecurity education on information security practices in libraries.[15]

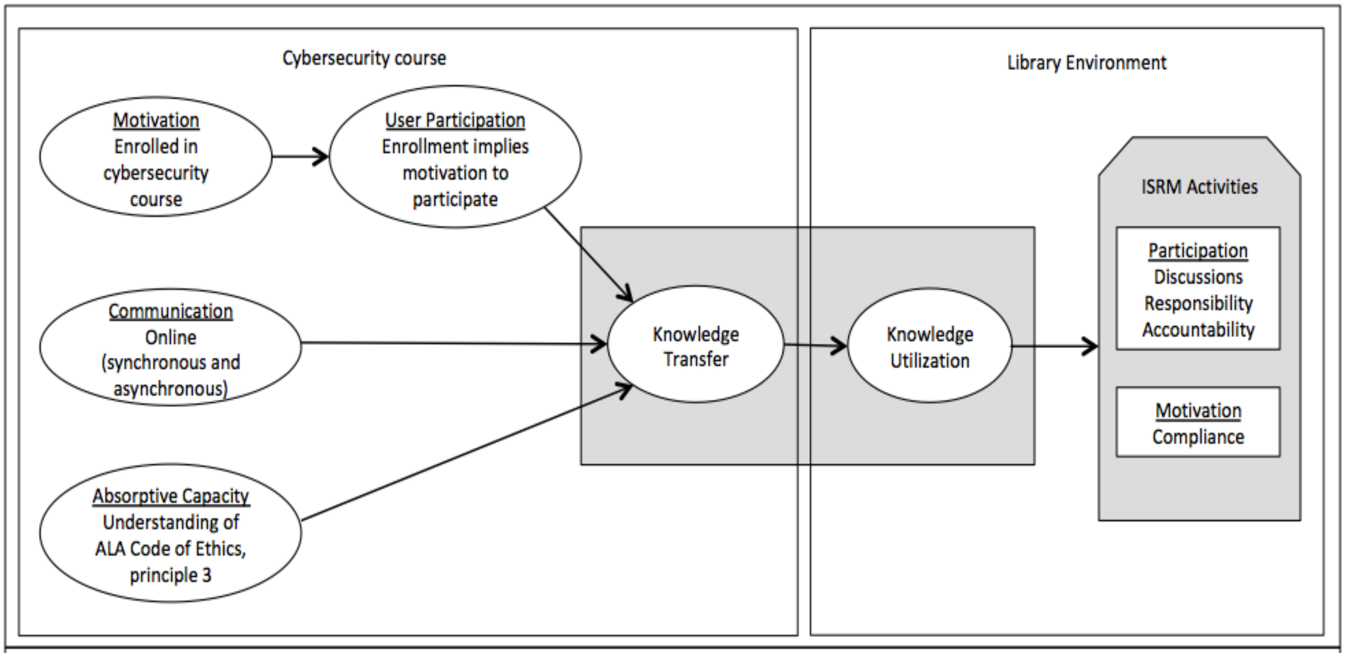

Figure 1. Factors of Knowledge Transfer Leads to Knowledge Utilization.

Absorptive Capacity

Absorptive capacity is the ability of a recipient to recognize the importance and value of eternally sourced knowledge, assimilate and apply it and has been found to be positively related to knowledge transfer.[16] Activating a student's prior knowledge could enhance their ability to process new information.[17] That is, knowledge transfer is more likely to take place between the instructor and students enrolled in a cybersecurity course if the student has existing knowledge or has had experience in some related area.

For the present study, students have stated that prior to enrolling in the cybersecurity course, they had little to no knowledge of cybersecurity. One student mentioned, "While I am the director of a small academic library, I have no understanding of cybersecurity. I am taking this course to learn about cybersecurity so that I can better secure the library I work in and to share the information with those who work in the library." Another student mentioned, "My goal is to work in a public library after graduation. I am taking this course because I keep hearing about cybersecurity breaches in the news, and I want to learn more about cybersecurity because I think it will help me in my future job." While all of the students enrolled in the course had no cybersecurity experience, all of them had some understanding of principle 3 in the ALA Code of Ethics, which states, "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted."[18] Understanding of principle 3 in the Code of Ethics demonstrates existing knowledge in some related area with regards to cybersecurity, albeit limited knowledge. Given this understanding, students should have the ability to process new information from the cybersecurity course.

Communication

The success of any SETA program depends on the ability of the instructor to effectively communicate the applicability and practical purpose of the material to be mastered, as distinguished from abstract or conceptual learning.[19] According to current research, knowledge transfer can only occur if communication is effective in terms of type, amount, competence, and usefulness.[20] For the present study, students were enrolled in an online graduate level cybersecurity course at a university we call Mountain View University (MVU). We changed the name to protect the privacy of the research participants. While research suggests that the best form of communication for knowledge transfer is face-to-face communication, the cybersecurity course at MVU is only offered online.[21] Therefore, communication relating to the course was conducted via course management software, email, video conferencing, discussion board, and pre-recorded videos.

Motivation

Motivation can be a significant influence on knowledge transfer.[22] That is, an individual's motivation to participate in SETA programs has been found to influence the extent to which knowledge is transferred.[23] Specifically, without motivation, a trainee may fail to use information shared with them about methods used to protect and safeguard patron privacy. In this present study, research participants voluntarily enrolled in the cybersecurity course. The cybersecurity course is not a core course or a class required for graduation. Therefore, enrolling in the course implies motivation to learn about cybersecurity by participating in course activities and completing assigned work.

User Participation

User participation in information security activities may influence effective knowledge transfer initiatives.[24] According to previous research, when users participate in cybersecurity activities, security safeguards were more aligned with organizational objectives and were more effectively designed and performed within the organization.[25] For the present study, given that students enrolled in the cybersecurity course, it is expected that they will participate in information security risk management activities, such as the completion of personal and organizational risk management projects.

CYBERSECURITY COURSE INFORMATION

This study will examine whether cybersecurity education strengthens information security practices within libraries. Based on the model in figure 1, students enrolled in the cybersecurity course (motivation), and therefore, were expected to participate in all course activities and complete assigned work (user participation), such as ISRM assignments. ISRM assignments are described in the Course Material section below. As per figure 2, the cybersecurity course was offered online, and used multiple forms of communication, including email, video conferencing, discussion board, and pre-recorded videos (communication). Students were able to access these resources through Canvas, a learning management system. Students came into the class with some understanding of principle 3 in the ALA Code of Ethics. Therefore, given that this knowledge is in a "related area," students may be able to process new information relating to cybersecurity (absorptive capacity). As per the above information and as depicted in figure 1, motivation, user participation, communication, and absorptive capacity will lead to knowledge transfer. Therefore, this study will focus on how knowledge transfer, as a means to strengthen information security, leads to knowledge utilization by cybersecurity students within information organizations.

Specifically, this study will explore the possibility of knowledge utilization leading to motivation, and participation in ISRM initiatives in libraries.

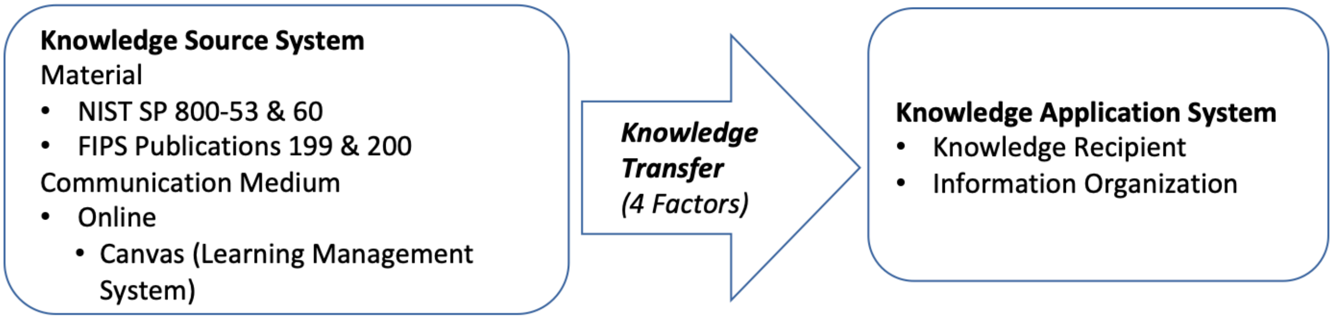

Figure 2. Knowledge Transfer Elements: Cybersecurity Knowledge Transfer for Information Organizations.

Course Material

The course was offered to graduate students at Mountain View University. Course material was created based on the National Institute of Technology Special Publication (NIST SP) 800-53 and 60, as well as Federal Information Processing Standards (FIPS) Publications 199 and 200. The focus of the course was information security risk management (ISRM). Course requirements included lab exercises, discussion posts relating to current cybersecurity findings and news reports, and ISRM assignments. ISRM assignments included a personal risk management assignment, which then led to the completion of an organizational risk management project (ORMP). Students completed the ORMP for various libraries, healthcare institutions, pharmaceutical companies, government organizations, and small businesses. With instructor approval, students were allowed to select the organization they wanted to work with. The objective of the course was for students to obtain an understanding of ISRM and be able to apply what they have learned to the workplace.

Course Communication

SETA programs depend strongly on the ability of the knowledge source to effectively communicate the importance and applicability of the knowledge shared. Current research suggests that the type of communication medium, relevance and usefulness of the information, and competency of the instructor can affect knowledge transfer. Given that face-to-face communication is considered the best method for successful knowledge transfer, it is important to understand if online communication methods were effective in the cybersecurity course described herein as the main focus of this study is to determine if knowledge transfer leads to knowledge utilization. According to table 1, respondents “Strongly Agree” or “Agree” that the materials used, relevance of communication, comprehension of instructor communication, and the amount of time communicating about cybersecurity in the course was effective (data collection described in section, Data Collection and Analysis.

	Response				
Questions	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
Medium: The material used in the cybersecurity course I took at MVU communicated security lessons effectively.	12 (50%)	12 (50%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
Relevance: Communication during the cybersecurity course I took at MVU was effective in focusing on things I needed to know about cybersecurity for my job.	10 (45.45%)	12 (54.55%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
Comprehension: In the cybersecurity course I took at MVU, the instructor's oral and/or written communication with me was understandable.	12 (54.55%)	10 (45.45%)	0 (0.00%)	0 (0.00%)	0 (0.00%)
Amount: In the cybersecurity course I took at MVU, the amount of time communicating about cybersecurity was sufficient.	12 (54.55%)	10 (45.45%)	0 (0.00%)	0 (0.00%)	0 (0.00%)

Table 1. Effectiveness of communication in cybersecurity course.

DATA COLLECTION AND ANALYSIS

The purpose of this study is to determine if knowledge transfer through cybersecurity education, as a means to strengthen information security, leads to knowledge utilization within libraries. Specifically, this study will examine if research participants will engage in ISRM activities after completion of the cybersecurity education course.

The model in figure 1 is examined via survey instrument by the authors. The survey instrument was available to former students who completed an online, semester long, cybersecurity course from fall 2013 through fall 2017. One hundred and twenty-six former students completed one of eight cybersecurity courses, and all were asked to participate in this study. Thirty-nine students accessed the survey, but only thirty-eight agreed to participate. Of those who agreed to participate in the survey, only twenty-two work in a library in the U.S. or a U.S. territory. Of the other sixteen participants, twelve do not currently work within a library environment, and four do not have a job. Therefore, responses from twenty-two research participants who work in a library in the U.S. or U.S. territory will be reported in this study. Table 2 provides a list of the types of libraries the twenty-two research participants work in.

Type of Library Environment	Response (22)
Academic Library	3 (13.64%)
Public Library	11 (50%)
School Library (K-12)	2 (9.09%)
Special Library	6 (27.27%)

Table 2. Types of libraries research participants work in.

Having knowledge and an understanding of information security policies, work processes, and information and information system use within a library environment, a knowledge recipient may understand the value of the knowledge shared with them through effective SETA programs and utilize the new knowledge to protect information and information resources. According to table 3, most survey participants stated that they have average to excellent knowledge of their library's computing-related policies, work processes that handle sensitive patron information, how access to patron information is granted, and how internal staff tend to use computing devices to access organizational information. A few respondents stated that their knowledge is below average.

	Response				
Questions:	**Excellent**	**Above Average**	**Average**	**Below Average**	**Poor**
How would you rate your knowledge of your organization's computing-related policies for internal staff computer usage?	4 (18.18%)	10 (45.45%)	8 (36.36%)	0 (0.00%)	0 (0.00%)
How would you rate your knowledge of your library's work processes that handle sensitive patron information?	4 (18.18%)	11 (50%)	6 (27.27%)	1 (4.55%)	0 (0.00%)
Within the organization you work for, how would you rate your knowledge of how access to patron information is granted?	3 (13.64%)	12 (54.55%)	5 (22.73%)	2 (9.10%)	0 (0.00%)
How would you rate your knowledge on how internal staff tend to use computing devices to access organizational information?	2 (9.10%)	11 (50%)	8 (36.36%)	1 (4.55%)	0 (0.00%)

Table 3. Knowledge of organization's computing-related policies.

Knowledge Transfer

For this study, knowledge transfer is measured as the extent to which the cybersecurity student acquired knowledge or understands the key educational objective. According to table 4 below, all survey participants stated that during the cybersecurity course, they acquired knowledge on information security risks, and solutions to manage information security risks within organizations. Furthermore, 91 percent of the twenty-two survey participants stated that they gained an understanding of the feasibility to implement solutions and potential impact of not implementing solutions to manage information security risk within the organizations in which they work. This is consistent with previous research that has measured knowledge transfer.[26]

Question: During the cybersecurity course I took at MVU, I ________.	**Response**
acquired knowledge on information security risks within the organization.	22 (100%)
acquired knowledge on solutions to manage information security risks identified within my organization.	22 (100%)
gained an understanding of the feasibility to implement solutions to manage information security risks identified within my organization.	20 (90.90%)
gained an understanding of the potential impact of not implementing solutions to manage information security risks identified within my organization.	20 (90.90%)

Table 4. Indicators of Knowledge Transfer.

Knowledge Utilization

The desired outcome of knowledge transfer is knowledge utilization.[27] This study is interested in the extent to which cybersecurity students have been engaged in information security risk management initiatives in their workplace since the completion of the cybersecurity course. According to table 5, twelve of the twenty-two survey participants have utilized the knowledge transferred to them from the cybersecurity course within the libraries in which they work. Of the twelve survey participants, ten performed security procedures within the organization on an ad hoc, informal basis. Seven worked on defining new or revised security policies. Four implemented new or revised security procedures for organizational staff to follow, and two evaluated at least one security safeguard to determine whether it is being followed by organizational staff.

Question: Since the completion of the cybersecurity course I took at MVU, I have _____ (please check all that apply).	**Response**
performed security procedures within the organization on an ad hoc, informal basis.	10 (83.33%)
worked on defining new or revised security policies.	7 (58.33%)
implemented new or revised security procedures for organizational staff to follow.	4 (33.33%)
evaluated at least one security safeguard to determine whether it is being followed by organizational staff.	2 (16.66%)
NOT performed any security procedures within the organization.	10 (45.45%)

Table 5. Indicators of knowledge utilization in the library.

Participation

Knowledge transfer through cybersecurity education may influence a cybersecurity student to utilize the knowledge they have gained by participating in ISRM activities. According to table 6, sixteen of the twenty-two survey participants have participated in ISRM activities in the library in which they work since the completion of the cybersecurity course. Fifteen communicated with internal senior management on training materials. Seven performed a policy review and communicated with internal senior management on training materials. Five worked on a security questionnaire, one had an interview with an external collaborator, and another research participant analyzed their library's business or IT process workflow.

Question: Since the completion of the cybersecurity course you took at MVU, have you performed any of the following activities within the workplace: (please check all that apply)	**Response**
Security questionnaire	5 (31.25%)
Interview with external collaborator (i.e. trainers)	1 (6.25%)
Policy review	7 (43.75%)
Business or IT process workflow analysis	1 (6.25%)
Communication with internal peers or staff on training materials	15 (93.75%)
Communicate with internal senior management on training materials	7 (43.75%)
I have NOT performed any security activities in my workplace	6 (14.29%)

Table 6. Participation in ISRM activities.

Participation may also include discussions on ISRM activities. According to table 7, sixteen of the twenty-two survey participants have participated in discussion on ISRM activities within the libraries they are currently working at. Fifteen survey participants participated in discussions on physical security, and ten had discussions on password policy. Seven survey participants had discussions on user provisioning, and six had discussions on encryption. Four survey participants had discussions on mobile devices, and another four had discussions on vendor security

Question: Since the completion of the cybersecurity course you took at MVU, have you participated in discussions on the following areas of security? (Check all that apply)	**Response**
Password policy	10 (62.5%)
User provisioning (i.e., establishing or revoking user logons and system authorization)	7 (43.75%)
Mobile device	4 (25%)
Encryption	6 (37.5%)
Vendor security	4 (25%)
Physical security	15 (93.75%)
Disaster recovery, business continuity, or security incident response	6 (37.50%)
I have NOT participated in any discussions relating to security in my workplace	6 (27.27%)

Table 7. Participation in discussions on ISRM activities.

Participation in cybersecurity education may lead to formal responsibility or accountability of ISRM activities. According to table 8, nine of the twenty-two survey respondents stated that since the completion of the cybersecurity course, they are formally responsible or accountable for ISRM in the libraries in which they work. Three research participants are responsible for identifying organizational members to participate in cybersecurity training. Five survey participants stated that they are responsible for communicating results on cybersecurity training to upper management, peers, and staff. Three research participants are responsible for organizational compliance with government regulations. Two are responsible for communicating organizational risk to the board of directors, and one research participant is responsible for organizational compliance of funder requirements.

Question: Since the completion of the cybersecurity course you took at MVU, are you formally responsible or accountable in the following ways? (Check all that apply)	**Response**
Identifying organizational members to participate in cybersecurity training	3 (33.33%)
Communicating results to upper management	5 (55.56%)
Communicating results to peers or staff	5 (55.56%)
Responsible for organizational compliance of funder requirements	1 (1.11%)
Responsible for organizational compliance with government regulations	3 (33.33%)
Responsible for internal audit	0 (0%)
Responsible for communicating organizational risk to the board of directors	2 (22.22%)
I am NOT formally responsible for security in my workplace	13 (59.10%)

Table 8. Participation via accountability of ISRM activities.

Motivation

An objective of SETA programs is to motivate knowledge recipients to comply with information security policies that serve to protect information and information resources. As such, cybersecurity education may motivate students to comply with organizational information security policies that serve to protect information and information resources. According to table 9, since the completion of the cybersecurity course, eighteen of the twenty-two survey participants stated that they believe it is important to protect patron sensitive data. Two respondents stated that they wholeheartedly feel responsible to protect their patrons from harm, and another two stated that they would be embarrassed if their organization experienced a data breach.

Since the completion of the cybersecurity course I took at MVU, ________.	**Response**
I wholeheartedly feel responsible to protect our patrons from harm.	2 (9.10%)
I believe it is important to protect our patrons' sensitive data.	18 (81.82%)
I would be embarrassed if my organization experienced a data breach.	2 (9.10%)
my job could be in jeopardy if my organization were to experience a data breach.	0 (0.00%)
I do NOT care about cybersecurity in my organization.	0 (0.00%)

Table 9. Motivation to protect patron privacy.

DISCUSSION

The purpose of this study was to evaluate the effects of knowledge transfer as a means to strengthen information security within libraries. Given the results from the survey instrument, the findings suggest that knowledge transfer through cybersecurity education can lead to knowledge utilization. Specifically, knowledge transfer through cybersecurity education may influence a library employee to utilize the knowledge they have gained by participating in discussions about, and the accountability and responsibility of ISRM activities. In addition, participating in SETA programs.

SETA programs are implemented within organizations as a means to increase compliance of information security policies. The findings suggest that library employees who completed a cybersecurity education course believe that it is important to, or feel that they have a responsibility to, protect patron private information. A couple of research participants stated that they would feel embarrassed if their organization experienced a data breach.

A student enrolled in a cybersecurity education course may develop an understanding of and value the information that is passed on from the knowledge source about ISRM activities. With ongoing development and implementation of SETA programs, activating a student's prior knowledge of ISRM activities could enhance their ability to process new information and apply to their job.

LIMITATIONS AND FUTURE RESEARCH

This research was conducted based on an online cybersecurity course offered at a university located in the western U.S. Therefore, future research is needed to study how cybersecurity courses in other parts of the U.S and internationally affects knowledge transfer as a means to strengthen ISRM initiatives in libraries, and other information organizations. It would also be valuable to conduct a modified version of this research within a classroom-based, face-to-face cybersecurity course. Furthermore, SETA programs implemented in libraries in the United States and internationally would add to this research area. There were 126 potential research participants identified, and although all were asked to participate, only thirty-eight completed the online survey. Of the thirty-eight completed surveys, responses from twenty-two participants were reported in this article. Participation from additional research participants may have generated different results.

While a major limitation of this study is its small pilot study and exploratory focus, a next phase of research should further investigate what type of SETA programs would be most effective in different library environments. While cybersecurity education may not be feasible for all library employees to obtain, examining and implementing the most effective SETA program for each library environment could strengthen cybersecurity practices in libraries across the U.S. A future study instrument should take into account the factors that influence knowledge transfer (absorptive capacity, communication, motivation, and user participation) as a means to strengthen ISRM practices. A common an important outcome for SETA programs is user compliance to information security policies. As such, a future study should test library employee knowledge of, and compliance to, information security policies.

CONCLUSION

U.S. libraries handle sensitive patron information, including personally identifiable information and circulation records. With libraries providing services to millions of patrons across the United States, it is important that they understand the importance of patron privacy and how to protect it. This study investigated how knowledge transferred within an online cybersecurity education course as a means to strengthen information security risk management affects library employee information security practices. The results of this study suggest that knowledge transfer does have a positive effect on library employee information security and risk management practices.

REFERENCES

[1] "Public Library Survey (PLS) Data and Reports," Institute of Museum and Library Services, Retrieved on June 10, 2018 from https://www.imls.gov/research-evaluation/data-collection/public-libraries-survey/explore-pls-data/pls-data.

[2] "Policy concerning Confidentiality of Personally Identifiable Information about Library Users," American Library Association, July 7, 2006, http://www.ala.org/advocacy/intfreedom/statementspols/otherpolicies/policyconcerning; "Professional Ethics," American Library Association, May 19, 2017, http://www.ala.org/tools/ethics.

[3] "Privacy: An Interpretation of the Library Bill of Rights," American Library Association, amended July 1, 2014, http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.

[4] Ibid.

[5] "Policy concerning Confidentiality of Personally Identifiable Information about Library Users," American Library Association; "Code of Ethics of the American Library Association," American Library Association, amended Jan. 22, 2008, http://www.ala.org/advocacy/proethics/codeofethics/codeethics.

[6] "Policy concerning Confidentiality of Personally Identifiable Information about Library Users," American Library Association; "Code of Ethics of the American Library Association," American Library Association.

[7] "Privacy: An Interpretation of the Library Bill of Rights," American Library Association.

[8] Samuel T.C. Thompson, "Helping the Hacker? Library Information, Security, and Social Engineering," *Information Technology and Libraries* 25, no. 4 (2006): 222-25, https://doi.org/10.6017/ital.v25i4.3355.

[9] Roesnita Ismail and Awang Ngah Zainab, "Assessing the Status of Library Information Systems Security," *Journal of Librarianship and Information Science* 45, no. 3 (2013): 232-47, https://doi.org/10.1177/0961000613477676.

[10] Ibid.

[11] Shayna Pekala, "Privacy and User Experience in 21st Century Library Discovery," *Information Technology and Libraries* 36, no. 2 (2017): 48–58, https://doi.org/10.6017/ital.v36i2.9817.

[12] Tonia San Nicolas-Rocca, Benjamin Schooley and Janine L. Spears, "Exploring the Effect of Knowledge Transfer Practices on User Compliance to IS Security Practices," *International Journal of Knowledge Management* 10, no. 2, (2014): 62-78, https://doi.org/10.4018/ijkm.2014040105; Janine Spears and Tonia San Nicolas-Rocca, "Knowledge Transfer in Information Security Capacity Building for Community-Based Organizations," *International Journal of Knowledge Management* 11, no. 4 (2015): 52-69, https://doi.org/10.4018/IJKM.2015100104.

[13] Dong-Gil Ko, Laurie J. Kirsch and William R. King, "Antecedents of Knowledge Transfer from Consultants to Clients in Enterprise System Implementations," *MIS Quarterly* 29, no. 1 (2005): 59-85, https://doi.org/10.2307/25148668.

[14] Spears and San Nicolas-Rocca, "Knowledge Transfer in Information Security Capacity Building for Community-Based Organizations," pp. 52-69; Dana Minbaeva et al., "MNC Knowledge Transfer, Subsidiary Absorptive Capacity and HRM," *Journal of International Business Studies* 45, no. 1 (2014): 38-51, https://doi.org/10.1057/jibs.2013.43; Geordie Stewart and David Lacey, "Death by a Thousand Facts: Criticising the Technocratic Approach to Information Security Awareness," *Information Management & Computer Security* 20, no. 1 (2012): 29-38, https://doi.org/10.1108/09685221211219182; Mark Wilson et al., "Information Technology Training Requirements: A Role-and Performance-Based Model" (NIST Special Publication 800-16), National Institute of Standards and Technology, (2018), https://www.nist.gov/publications/information-technology-security-training-requirements-role-and-performance-based-model; San Nicolas-Rocca, Schooley and Spears, "Exploring the Effect of Knowledge Transfer Practices on User Compliance to IS Security Practices," 62-78.

[15] Spears and San Nicolas-Rocca, "Knowledge Transfer in Information Security Capacity Building for Community-Based Organizations," 52-69.

[16] Janine L. Spears and Henri Barki, "User Participation in Information Systems Security Risk Management," *MIS Quarterly* 34, no. 3 (2010): 503-22, https://doi.org/10.2307/25750689; Piya Shedden, Tobias Ruighaver, and Atif Ahmad, "Risk Management Standards-the Perception of Ease of Use," *Journal of Information Systems Security* 6, no. 3 (2010): 23–41.

[17] Shedden, Ruighaver and Ahmad, "Risk Management Standards-the Perception of Ease of Use" pp. 23-42; Janne Hagen, Eirik Albrechtsen, and Stig Ole Johnsen, "The Long-term Effects of Information Security e-Learning on Organizational Learning," *Information Management & Computer Security* 19, no. 3 (2011): 140-154, https://doi.org/10.1108/09685221111153537.

[18] "Code of Ethics of the American Library Association," American Library Association.

[19] Spears and San Nicolas-Rocca, "Knowledge Transfer in Information Security Capacity Building for Community-Based Organizations," pp. 52-69; Wilson et al., "Information Technology Training Requirements: A Role- and Performance-Based Model" (NIST Special Publication 800-16).

[20] Thompson S.H. Teo and Anol Bhattacherjee, "Knowledge Transfer and Utilization in IT Outsourcing Partnerships: A Preliminary Model of Antecedents and Outcomes," *Information & Management* 51, no. 2 (2014): 177–86, https://doi.org/10.1016/j.im.2013.12.001; Ko, Kirsch, and King, "Antecedents of Knowledge Transfer from Consultants to Clients in Enterprise System Implementations," 59-85; Minbaeva et al., "MNC Knowledge Transfer, Subsidiary Absorptive Capacity and HRM," 38-51; Geordie Stewart and David Lacey, "Death by a Thousand Facts: Criticising the Technocratic Approach to Information Security Awareness," *Information Management & Computer Security* 20, no. 1 (2012): 29-38, https://doi.org/10.1108/09685221211219182.

[21] Martin Spraggon and Virginia Bodolica, "A Multidimensional Taxonomy of Intra-firm Knowledge Transfer Processes," *Journal of Business Research* 65, no. 9 (2012) 1,273-282: https://doi.org/10.1016/j.jbusres.2011.10.043; Shizhong Chen et al., "Toward Understanding Inter-organizational Knowledge Transfer Needs in SMEs: Insight from a UK Investigation," *Journal of Knowledge Management* 10, no. 3 (2006): 6-23, https://doi.org/10.1108/13673270610670821.

[22] Maryam Alavi and Dorothy E. Leidner, "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues," *MIS Quarterly* 25, no. 1 (2001): 107-36, https://doi.org/10.2307/3250961.

[23] Ko, Kirsch, and King, "Antecedents of Knowledge Transfer from Consultants to Clients in Enterprise System Implementations," 59-85.

[24] San Nicolas-Rocca, Schooley, and Spears, "Exploring the Effect of Knowledge Transfer Practices on User Compliance to IS Security Practices," 62-78; Spears and San Nicolas-Rocca, "Knowledge Transfer in Information Security Capacity Building for Community-Based Organizations," 52-69.

[25] Spears and San Nicolas-Rocca, "Knowledge Transfer in Information Security Capacity Building for Community-Based Organizations," 52-69; Spears and Barki, "User Participation in Information Systems Security Risk Management," 503-22.

[26] San Nicolas-Rocca, Schooley, and Spears, "Exploring the Effect of Knowledge Transfer Practices on User Compliance to IS Security Practices," 62-78; Janine L. Spears and Tonia San Nicolas-Rocca, "Information Security Capacity Building in Community-Based Organizations:

Examining the Effects of Knowledge Transfer," 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, 2016, pp. 4,011-20, https://doi.org/10.1109/HICSS.2016.498; Ko, Kirsch, and King, "Antecedents of Knowledge Transfer from Consultants to Clients in Enterprise System Implementations," 59-85.

[27] Ko, Kirsch, and King, "Antecedents of Knowledge Transfer from Consultants to Clients in Enterprise System Implementations," 59-85; Teo and Bhattacherjee, "Knowledge Transfer and Utilization in IT Outsourcing Partnerships: A Preliminary Model of Antecedents and Outcomes," 177–86.