International Journal of Business and Management; Vol. 18, No. 4; 2023
ISSN 1833-3850 E-ISSN 1833-8119
Published by Canadian Center of Science and Education

Cybersecurity Training in Organization as Human Capital Investment: A Qualitative Grounded Theory Analysis

Yuying Shen[1], Carlene Buchanan Turner[1] & Claude Turner[2]

[1] Department of Sociology, Norfolk State University, Norfolk, USA

[2] Department of Computer Science, Norfolk State University, Norfolk, USA

Correspondence: Yuying Shen, Ph.D., Associate Professor, Department of Sociology, Norfolk State University, Norfolk, VA, 23504, USA. E-mail: yshen@nsu.edu

Received: March 16, 2023 Accepted: April 25, 2023 Online Published: May 26, 2023

doi:10.5539/ijbm.v18n4p38 URL: https://doi.org/10.5539/ijbm.v18n4p38

Abstract

This study aims to examine the impacts of organization's cybersecurity training program on employees with qualitative data, collected from 33 college students who were attending Norfolk State University while also working either on a part-time or full-time basis participated. Open-ended questions were asked to elicit participants' perspectives on cybersecurity training and cybersecurity protocols in organizations. Using qualitative data analysis software *Nvivo* 12*,* the authors organized and analyzed the collected data with open coding, and selective coding to recognize the major influencing impacts from cybersecurity training on employees' routine work and behavior. Inductive and grounded theory analysis further elaborates connections between employee's cybersecurity training and efficiency of organizations. Our findings suggest that on-the-job cybersecurity training provided by the employer is an effective investment for modern organizations to build on the organizational human capital and consequently to improve the efficiency of the organization. Findings from this study corroborates with the tenet of human capital theory that on-the-job educational program or training is economical and effective to manage the human capital challenge for modern organizations.

Keywords: Qualitative Interview, Grounded Theory Analysis, Cybersecurity Training, Organization, Efficiency

1. Introduction

Many day-to-day activities needed for the operation of modern organizations nowadays are increasingly dependent on the digital platforms and systems, which makes organizations be more susceptible for cybersecurity breaches. Cybersecurity breaches are increasingly prevalent and are bringing devastating impacts to organizations attacked as well as the national economy and security (Cashell et al., 2004). For example, there has been a 782% increase in the number of reported cyber-attacks against federal agencies from 2006 to 2012 in the U.S. (Oce, 2013; Hirshfield et al., 2015). Compared to 2020, there were 50% more cyberattacks per week on corporate networks in 2021 (Brooks, 2022). In addition, according to the 2021 IBM data breach report (IBM Security, 2021), data breach costs have also significantly grown year by year, increasing from $3.86 million in 2021 to $4.24 million in 2022. Cyber risks continue to top worldwide business challenges in 2022 (Brooks, 2022).

The continuous prevalence of largescale information breaches from both the public and private organizations as well as the consequently evolving damages and threats in the cyber landscaping requires organizations at different levels to develop strategies to mitigate the threat and vulnerability (Nobles, 2018). Millions of dollars have been spent on new technologies to secure the cyberspace. Just an extensive cybersecurity infrastructure with all up-to-date technology in place, however, cannot ensure the cybersecurity (van Zadelhoff, 2016). Much like almost any aspect of an operation, cybersecurity comes down to one simple tenet: It will only be good when the people who are tasked with it can make it work on a day-to-day basis. It is the people with the right knowledge, skills, and abilities to implement those technologies who will determine the success of cybersecurity defense (Brooks, 2022; Hirshfield et al., 2015).

Human actor in cybersecurity is critical to respond to cybersecurity challenge (He & Zhang, 2019; Vieane et al., 2016). Even with the best-laid cybersecurity plans being in practice in organizations, if the employees are ignoring policies, the best-laid plans or protocols would plunge onto the ground suddenly. It is reported that 95%

of the cybersecurity breaches are attributed to human errors and actions from the people's routine task such as an employee's click of a phishing email (Brooks, 2022). Disparaging organizational losses resulted from the errors of human factors in information protection, including bankrupt reputation, business losses, and government sanctions, have also been increasingly reported (van Zadelhoff, 2016).

A highly trained, motivated workforce is needed to help protect security and data of the organizations. However, there are not enough cybersecurity experts. With a critical shortage of trained cybersecurity professionals available, how to protect the information assurance and cybersecurity of organizations is a daunting challenge. Such cybersecurity challenge is even urgent for small and medium-sized business, which account for 43% of all data breaches while at the same time they are more likely to be underprepared for cybersecurity without a plan in place (Hirshfield et al., 2015). A technically skilled and cyber-savvy workforce knowledgeable for the proper cybersecurity procedures are therefore needed to be the last line of cyber defense to ensure the future cybersecurity. It is therefore imperative for organizations to build a model of cybersecurity culture to educate employees' security awareness and cultivate their capabilities to engage in safe cybersecurity behaviors (Anwar, He, Ash, et al., 2016; Huang & Pearlson, 2019; Kweon et al., 2021).

Fostering proper cybersecurity awareness among employees from organizations at different levels to reduce the susceptibility of cybersecurity breaches and the consequent losses is widely discussed (Huang & Pearlson, 2019; Zhang et al., 2021). Cybersecurity training and education for employees, focusing on recognizing the potential cybersecurity threats and the appropriate actions to take to reduce risks proactively, has been recommended as an effective method for cultivating cybersecurity skills and combatting cyberattacks (He & Zhang, 2019). Despite the growing interests in the importance and necessity of the cybersecurity training, due to the absence of referential studies, many organizations are still cautiously hesitating in making decisions to arrange optimal security training programs for their employees (Kweon et al., 2021). In addition, existing studies of cybersecurity in organizations mainly focus on technological aspects but with insufficient attention on human factors (Schultz, 2005; Vieane et al., 2016).

Understanding the development of employees' productive and proper security-centered behavior is very important in information security research and organization study (Huang & Pearlson, 2019; Li et al., 2019; Schultz, 2005). Majority studies on cybersecurity training for employees mainly adopt a technical perspective to emphasize the contribution of cybersecurity training programs in building cybersecurity culture by improving employees' cybersecurity risk perception and cybersecurity behaviors, with evidence from quantitative research design (Alshaikh, 2020; He et al., 2020; Kweon et al., 2021). A recent study by Reeves et al. (2021), however, has presented a multidisciplinary perspective to illustrate the existence of cybersecurity fatigue in workplaces. Further research is still needed to reveal the nuances and intricacies of different aspects of cybersecurity training in an organizational context. This study aims to bring in the human factors in cybersecurity research by empirically revealing the impacts of cybersecurity training in organizations from a sociological perspective. It examines the potential impacts of cybersecurity training on employees and employers, based on qualitative in-depth interview among a group of college students, who are in the line for future employment and all of them are also working in different organizations on a part-time or full-time basis. Their perceptions and experiences of cybersecurity training and how such training is impacting their routine work and benefiting the organizations is revealed with their own words. The result of this study can be used as a referential guide for information security training decision-making procedure as well as the efficiency improvement strategy framework in modern organizations.

2. Methods

2.1 Research Design & Study Subjects

This study designs a qualitative research method to explore the perceptions of cybersecurity training in organizations among a group of college students, who are the future workforce in line and all of them were also working in different organizations or agencies when they were interviewed.

Intensive interview with open-ended questions was used to collect data from 33 college students, who were attending Norfolk State University for undergraduate or graduate programs between 2021 and 2022. The participants were selected using purposive sampling method to recruit study subjects who meet specific criteria regarding the study topic. The criteria used in this study include: (1) was registered in undergraduate or graduate programs at Norfolk State University, an HBCU in Virginia, U.S., (2) was working in an organization or agency either on a part-time or full-time basis; (3) had completed one of the following organization-related courses at Norfolk State University: Sociology of Complex Organization, Organizational Behavior, Management of Information Security, and Urban Organization Administration.

Participating students were recruited with the solicitation through social media, posters, and flyers. A brief introduction of the research project was provided at the beginning. Informed consents from the participating students were obtained prior to enrollment in the interview, in which they indicated their willingness to participate in the interview. Participation in the interview was voluntary. Participants were also told that they could skip any questions that they did not want to answer. In total, 33 students from 9 academic programs at NSU participated in interviews. The Institutional Review Board Committee at Norfolk State University approved the sampling procedures, strategies for preserving confidentiality and anonymity, and the interview questionnaire used in this study.

Table 1 presents demographic characteristics of the sample in this study and their baseline cybersecurity knowledge. Male participants outnumbered the female participants in this study. Most of our study subjects were younger than 30. Majority of our participants (70%) knew the basic cybersecurity protocols in organizations and acknowledged the importance of cybersecurity training in organizations. In addition, most participants (85%) agreed that cybersecurity training for employees was important for the successful operation of modern organizations.

Table 1. Characteristics of respondents (N = 33)

	Frequency	**Percentage (%)**
Gender		
Male	14	42%
Female	19	58%
Age		
Younger than 30	24	73%
30 and above	9	27%
Educational Level		
Undergraduate	21	64%
Graduate	12	36%
Require cybersecurity training		
Yes	28	85%
No/not sure	5	15%
Cybersecurity Knowledge		
Good	26	79%
Poor	7	21%
Total	**33**	**100%**

2.2 Data Collection

Data were collected with in-depth interviews conducted individually for each respondent on Zoom from August 2020 to August 2021. Interviewers followed the same set of open-ended questions for all respondents. Interview questions focused on interviewee's perceptions of the importance of cybersecurity training in organizations, the potential impacts of cybersecurity on employees. Specifically, the following questions were asked to tap their perceptions of the cybersecurity training protocol in organizations: Is cybersecurity important to organizations? Should all employees have cybersecurity training? Where do most regular employees get their cybersecurity training? Why do companies have cybersecurity rules/protocols? What are some of the major cybersecurity rules in organizations/companies? How does cybersecurity training impact the employees' routine daily work? How does cybersecurity training impact the employees' coordination with others? Respondents' background knowledge of the currently popularized major cybersecurity protocols and popular cybersecurity training components such as password management & two-factor authentication, phishing or social engineering, encouraging email vigilance, raising awareness of phishing, remote access and network access training, cloud security training, social media security training avoiding personal devices for work, computer hardware security, and using a virtual private network (VPN), were also tapped.

In addition, several demographic questions were asked about the respondent's gender, age, educational level. Interviews were conducted online via Zoom, with the interviewee's video being off to ensure confidentiality and privacy. The interviews were audio-recorded with the permission of the interviewees.

2.3 Data Analysis

The audio-recorded interviews were transcribed verbatim using the transcription service of qualitative research software *Nvivo* 12 by QSR International. *Nvivo* software was further used to house, organize, and analyze the data. Data presented in this study have been "cleaned up," with any false starts, any residual identifying information, and non-lexical utterance having been deleted for clarity and space.

In line with a standard approach to qualitative data analysis, we have read each transcript iteratively to ensure understanding of interview content. We then used *Nvivo* software to code the interview transcripts, relying on inductive analysis and grounded theory to conduct line-by-line open coding and selective coding. Inductive grounded theory analysis that emphasizes the dynamic construction of codes for the purpose of developing analytical and theoretical interpretation of data (Charmaz, 2006; Silverman, 2006) was followed. We first inductively identified the recurring patterns and conceptual categories as they emerged from the transcript. Following the grounded theory reasoning, human capital was then developed as the theoretical framework by connecting and comparing the key codes and themes from the transcripts. Two coders independently reviewed all cases to identify the main themes occurring in the respondents' interview. Once completed, we compared and checked the results, and all discrepant codes were discussed and reconciled.

This paper mainly focuses on the respondents' perspective of how cybersecurity training will impact the regular employees' performance and behavior in daily routine jobs. We therefore centered our analysis specifically on interviewee's perception of cybersecurity training in organizations, and how cybersecurity trainings were impacting employees' timely delivery of the routine job assignment, the predictability of behavior, and the coordination with others. First, the following codes were created to categorize data as it relates to cybersecurity training and cybersecurity protocols in organizations: on-the-job cybersecurity training; employees' timely delivery of routine work; employees' predictable behavior; team coordination. Codes were also created to categorize the respondents' demographic characteristics and their background knowledge of cybersecurity protocols. Transcripts were closely read and searched for narratives that implicitly or explicitly attributed to the basic codes. Conceptual memos were then created to develop categories and subcategories by putting together extracts that are related to each other into codes. A list of themes was developed to classify the themes of the transcripts.

3. Results

Our qualitative interview data provide respondents' accounts of whether cybersecurity training is necessary and how cybersecurity protocols will impact the routine job performance of employees. We took a broad view of cybersecurity training to include all training related to cybersecurity. Analyses of our empirically collected data revealed the following broad themes: (1) cybersecurity training as the responsibility of organizations; (2) on-the-job cybersecurity training in organizations will improve organizational efficiency by fostering trained behavior and creditable performance for employees.

3.1 Cybersecurity Training as the Responsibility of Organizations

When participants were asked directly whether cybersecurity training was important, majority of them were well cognizant of the importance of cybersecurity training. For example, as explained by one respondent: "You have a lot at stake when you have employees and people who aren't familiar with just even the basic security protocols you can do damage. Like I said, you can do a lot of damage."

Respondents were also asked about their perception of where employees should get cybersecurity training. Most of them regarded that employees should get cybersecurity training directly from their employers, with many implicitly or explicitly attributing cybersecurity training as the responsibility of organizations. Majority of them deemed that cybersecurity training should be integrated "on the job at work" and "something that's coming down through the company." And training should be at the very beginning of their employment in "the place of employment" and may be "either a class through IT department or a training online class." Typical responses such as the following ones further illustrate that majority of our respondents consented that organizations should take the responsibility of training their employees for cybersecurity protocols and the relevant knowledge.

"From my knowledge, if they're getting any training, it's something coming down through the company. So, if it's up to the organization to do their research and make sure they select the best that do available to them."

"It should be a class that's given to the employees through the employer."

"Most likely it would have to be from their jobs. Maybe. Yeah. The place of their employment, most likely. So yes. Place of employment."

"Training should be through the companies that we work for."

"I will believe it will come from their work force or where they work at."

A number of respondents who were also working confirmed that they "had cybersecurity training through" who they "were employed." Further, some respondents believed that cybersecurity training should be mandatory. For example, one respondent said the following words:

"If I had to guess, it's probably from the company themselves in terms of the basics. Here is some of the some of the most common things that to expect. And this is mandatory training before you start working here."

One challenge in cybersecurity is that cybersecurity is never static. Everything involved with cybersecurity is always changing and evolving, including the threats, the systems, the applications, the attacks, the protecting countermeasures as well as the people who are using the system and technology (Tommey, 2018). As threats evolve, the cybersecurity approach must evolve, and employees need to stay abreast of new solutions and be willing to implement them in an effective way. So, a continuous improvement style approach is expected for cybersecurity in organizations (Tommey, 2018). Based on the interview transcripts, our respondents were aware of this challenge. Our respondents agreed that regular training will not "disrupt the organization" and should not be taken as a burden. They believed that "it is in the organization's best interest to have regular training for its staff" and "companies should definitely be training their employees in terms of ensuring like ensuring them that their knowledge is up to date and it's up to par with how they can." The training information "can be regularly sent out to the employees in monthly newsletter." Some other typical responses as the follows concur with the similar opinion that cybersecurity training should be offered and updated regularly:

"I think most regular employees get their information from their IT department, newsletters coming at, you know, their monthly newsletter or the news."

"We have to do monthly security awareness videos and security awareness shows, so employees pretty much get their training from their jobs."

"I would say most of it could be from like on boarding training. It's like if you start a new job and the onboarding process where you do like your learning modules or, you know, whatever, and they go watch this video of, you know, how to protect your information, you know, like lock your computer and stuff like that, just like the basics."

"I believe it is in the organization's best interest to have regular training for its staff. I mean, you know, sometimes people get tired of having ongoing trainings, but I don't look at it as a way of disrupting the organization. I think more training of these things are, for example, one of the ways that can improve Cybersecurity rules."

A research study from 2014 Enterprise Management Associates (EMA) reported that 56% of personnel, not including IT and security staff, have not received any security awareness training in their organizations. With the broad discussion of the importance of cybersecurity, a study from 2021 (Sabillo et al., 2021) indicates that promoting cybersecurity awareness is still needed. company size, market and budgets have a significant impact on the existence and maturity of their corporate awareness training (Sabillo et al., 2021). Cybersecurity training programs are therefore not available in some companies. Our study also finds that promoting cybersecurity awareness is still needed. One respondent who was working on a part-time basis at a call center said that "I work at a call center on weekends and they (employers) gave us cybersecurity training and they(employer) paid for it." However, a very small number of respondents did think that some jobs may not necessarily need cybersecurity training. For example, as explained by the following responses:

"No, I don't think it's necessarily important for that, because if you work in sales and or even real estate, why would I be cybersecurity training? You know, I'm saying so at the end of the day, I think it just depends on the type of career path you're going down or the type of career path that you're interested in."

"I believe everyone should get the right amount of training to do their specific job, but they don't need it for this specific job. And it's really no purpose to get that type of training."

3.2 Cybersecurity Training Increase Organizational Efficiency by Improving Employees' Behavior & Performance

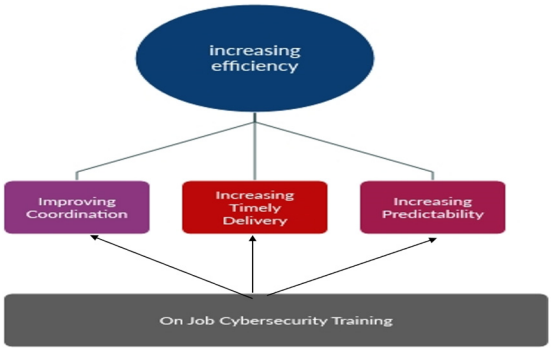

Figure 1. On-the-Job cybersecurity training helps improve organization's efficiency

We also asked respondents' perceptions of how cybersecurity training was impacting employees' behavior and performance in their daily routine jobs. There were some variations in participants' responses. But taken together, the overall impression was that they all pointed to the improvements in employee's behavior and performance and team coordination in organization, as illustrated in Figure 1. Most participants' narratives suggested that on-the-job cybersecurity training in organizations would promote the timely delivery of the job assignments, increase the predictability of employees' behavior, and foster coordination with team members. All of which are crucial for improving the efficiency of the organizations. As one respondent said,

"Oh yes definitely, I feel like it's a big impact because it's good to have knowledge on all the cyber, you know, cybersecurity awareness, you have the knowledge that can be passed on, not just one person having knowledge. You know, everybody shares the same knowledge because they say knowledge is power. So, by people sharing knowledge, I mean everybody in your team have the same knowledge… it creates a bigger, you know, cyber security where the whole company is just like everybody knows a lot about it and they can easily protect the company, you know, when that threat comes because everybody is knowledgeable on that level."

Other responses similarly concurred the positive impacts of cybersecurity training on team coordination by making all team members "on the same page" to "improve the workflow of the team." For example, our participants also told the following scenarios:

"So, it was flagged for phishing, and it was deemed correct. So, you know, other employees that did not notice that would have clicked that and, you know, it could have impacted the company. So, awareness across the team does make a difference. So everybody should be kind of like on the same page when it comes to security rules."

"If you're working in a team within your organization, I believe that knowledge of cybersecurity practices and, of course, risks of cyber attacks would benefit the team and if team members are all aware of the cyber threats and they possess the same knowledge about cyber security risks and what you should watch out for, I think it would actually improve the workflow of that team."

"But whatever you're trying to accomplish is to get done if you're not following the rules and then it's not allowing the task to flow correctly. The team I feel like you have to. Cybersecurity employees, everybody should be following the rules of what is in front of them."

Cybersecurity training in organizations promotes synchronized and skillful team coordination, which is essential for the successful operation of the organization. One respondent said that "I think having a strong team or with like that knows the policies, knows the knowledge, makes everything smoother and it gets things done faster and there's less clutter and confusion when trying to address issues across the company." And on-the-job cybersecurity training from the employer will ensure greater team coordination since "if everyone on the team is doing training and everyone around understand everything related to those cybersecurity procedures and policies. When something usual happens, I mean those related to cybersecurity, team members will be aware and will know how to fix it. And company will be strong ultimately."

On-the-job cybersecurity training in organizations further promotes timely delivery of employees' routine job assignments and predictability of their behavior. One respondent regarded that if organizations provide "training opportunities for their people so they could be able to know how to go about their work." If the employees encounter some cybersecurity issues in their work or "a situation like that arise, they could be able to know how to go about it, what to do or where to get help." On-the-job cybersecurity training will make them

"knowledgeable to get some countermeasures immediately." It can offer employees technical solution that is secure and efficient to do their routine jobs. Lack of cybersecurity training may make the employees take more time to maneuver in their daily job in a disordered and inconsistent way, which might delay their job assignment delivery and trigger unpredictable uncertainty in their daily routine job.

On-the job cybersecurity training in organizations provides technological skills for employees to avoid cybersecurity breaches in their daily work, both for in-role and out-role work. In one respondent's words, "I think if you're fairly new to or, you know, if you haven't received that training and you are fairly new to working in an organization and may you know, it may take you a lot longer. To maneuver or at least recognize, you know, something suspicious."

Cybersecurity training programs in organizations also behavior change in their employees. Many respondents said that after they had completed the cybersecurity training program required by their employers, they became more "vigilant" "careful" "cautious" in "using social medias" and clicking emails from "someone [they]are not familiar or from someone not working in the same place." And they were "more likely to adapt their behaviors to follow their team members to be cyber-safe."

It further helps build a corporate culture proactive to secure teamwork and collaborative workplace. For example, one respondent said,

"Oh, I think that before establishing a team, you should go over that protocol, you know, that protocol to safety so that it doesn't necessarily affect the team's work or how they, you know, get things done efficiently. If everyone's on the same ground of understanding, then I think you'll be fine."

The same theme is illustrated in the following narratives:

"I believe it can help coordination if everybody is on the same page. They're all aware of the rules and or if they're all respecting those rules. I think having everybody on the same page and having knowledge and understanding of the cyber security rules, I think it allows for a more seamless and obviously secure experience."

"And it's not only you are able to work as a team, but as a team, you know, like you're doing the right thing on. As far as like, if one person knows something, another person doesn't know if another like you might be doing everything right to ensure the security of your system, but maybe somebody on your team is not doing something right and they could cause a breach or some mishap that affects everybody. So, I also think it's important to make sure that everybody on the team knows how to like, follow in and just maintain the cyber security procedures and protocols for everybody's safety and for the safety of the company."

Efficiency means the "optimum method for getting from one point to another" (Ritzer, 2013, p. 12). It connotes the selection of most favorable ways to achieve a desired result at the shortest time. Organization's cybersecurity training provided for their employees actually improves the efficiency of the organization by promoting everyone to pursue the optimal way to finish their job assignment.

4. Discussion

By analyzing interview data from our study subjects, this article demonstrates that cybersecurity training benefits the organization. Our study subjects concurred with their own words that cybersecurity training program will help mitigate cybersecurity vulnerabilities for organization and protect organization's critical assets from cyberattacks, exploitation, fraud, and employees' behavior, which is in line with previous studies (He & Zhang, 2019; Li et al., 2019; Miranda, 2018).

Analysis of qualitative interview data from our research further expands this line of cybersecurity study by suggesting that cybersecurity training for employees, in particular on-the-job cybersecurity training in organization, will boost its human capital from the bottom up to improve the efficiency of organization. It will strengthen the human capital of employees, both technical and non-technical ones. The job performance and efficiency of the whole team will be improved gradually. An agglomerate force will consequently be accumulated at the organization level to optimize the efficiency of the organization. On-the-job cybersecurity training is an effective way to manage the human capital challenge for modern organizations.

According to human capital theory, which was first conceptualized by economist and philosopher Adam Smith (1776), each individual employee embodies a set of resources which can be used by the individual, and/or employer to generate wealth or income (Smith, 1776; Teixeira, 2007). These resources can be the knowledge, talents, skills, abilities, experience, intelligence, training, and wisdom possessed individually and collectively (Pasban et al., 2016). Human capital is perceived to have a relationship with economic growth, productivity, and

profitability (Teixeira, 2007). Investment in human capital will lead to measurable benefits of productivity, profitability, and increased earnings because human capital contains the productive wealth embodied in skills and knowledge (Pasban et al., 2016).

For organizations, human capital is the productive capacity developed, embodied, and stocked in individual employees at the micro-level and the organization at the macro-level. Employers can improve the macro-level human capital by investing in the training and education of their employees to increase returns for both the individual and the larger economic system (Sweetland, 1996). New technologies always bring organizational changes by de-skilling employees (Boddy, 1996). The increasing integration of technologies in daily routine work in organizations requires formal knowledge and skills for the potentially empowering aspects of using new technologies in routine work. Training and educational program in organization develops human capital by providing a unique resource for skills and abilities to cope with cybersecurity risks actively and flexibly, avoid information breaches, and prepare for those that cannot be avoided. Training and educational program in organization further instills broadly effective habits and attitudes for employees' daily routine work, in addition to the cybersecurity related job assignment. Training and educational program in organization is a resource itself, and the learned effectiveness it represents helps employees generate further resources and human capital.

Human capital investment in employees increases their values to themselves and their employer (Rivera, 2020; Sweetland, 1996). Employers who invest in developing the human capital of their employees through work-based learning and on-the-job training receive benefits in the areas they invested in, including improved service for clients, production of quality products, employees' behavior predictability, and employees' speeded delivery of expected work (Rivera, 2000). How to develop human capital is therefore one of the most important determinants of organizational efficiency and performance.

Organization's efficiency and economic growth is heavily dependent on the growth in human capital because skills drive productivity, and competitiveness (Hanushek, Eric, & Woessmann, 2015). Work-based learning and on-the-job-training has long been recognized as one of the best ways to teach new skills, maximize knowledge retention, and quickly apply aforesaid skills and knowledge in a real-world work environment (Mühlemann, 2016; Tsang, 1997). On-the-job training will improve the participants' skills needed in the workplace, both cognitive and non-cognitive. It will further bring pecuniary and non-pecuniary benefits to the trainees. On-the-job training program also brings many benefits to the employers, including an increase in work productivity and a decrease in turnover rates (Tsang, 1997). It provides tangible and intangible benefits to direct and indirect participants, the employer and the greater community or society.

Analysis of the respondents' narratives in this study echoes with the tenets of human capital theory, expounding that on-the-job cybersecurity training is an important way to improve organization's efficiency by boosting the human capital at the individual, team, and organizational levels. As revealed in our respondents' narratives, on-the-job cybersecurity training upgrades employees' occupational skills as well as soft skills that can assist them in better navigating both the technical and the non-technical requirements, expectations, and responsibilities of their job and field.

These enhanced skills at the micro-level of individual employees can lead to further growth of human capital at the meso-level of working teams and gradually cluster at the macro-level of organization. Employees' behavior is learned and impacted by their team members, and they will learn and adapt quite quickly in work environment (He et al., 2016; Livingston, 2021). Narratives from our respondents further delineate how on-the-job cybersecurity training is helping improve the team coordination as well as tangible and non-tangible skills needed for other person-to-person interactions in organizations, which promote synchronized and skillful team coordination to ensure the successful operation of the organization.

The efficiency of a group working together is directly related to the homogeneity of the work they are performing, of the processes they are utilizing, and of the purposes which actuate them (Gulick, 1937; Ritzer, 2013). The success of modern bureaucratic organizations is mainly attributed to its operation along rational lines in a fixed and stable model that can be learned (Lippmann & Aldrich, 2003; Weber, 2009). With on-the-job cybersecurity training, the regular activities in workplace required for the purpose of cybersecurity are distributed in a fixed and stable way for all team members and keep them on the same page, which guarantee the regular and continuous fulfillment of these duties and for the execution of the corresponding rights. On-the-job cybersecurity training will promote adherence to the protocols of cybersecurity to reduce confusion, inefficiency and irresponsibility which arise from the violation of the principle. From bottom to top, the team finally will be unified in terms of cybersecurity operation.

On-the-job cybersecurity training in organizations impacts the predictability of employees' response to security

vulnerability. It will guide employees in their routine daily work. It further impacts the predictability of employees' response to other routine daily work. Employees' behavior is expected to be predictable because of standardization and homogenization of the mode of operations. Their behaviors are predictable because they follow rules and are guided by scripts; thus, what they do or say, how they will do or say it, is highly predictable (Ritzer, 2013). All will also increase the timely delivery of employees' expected job assignments.

On-the job-cybersecurity training promotes the already-made cybersecurity protocols to be followed in organizations. Conducting cybersecurity training in organizations implies the standardization of management mode in organizations, which will strengthen employees' willingness and commitment to following the cybersecurity protocols and rules. It further implies that there are formal rules and procedures to be followed in routine daily job and there are expectations to be fulfilled. Following standardized rules and homogeneous ways of cybersecurity operation, in technology or in purpose, will improve the predictability and streamline of the required responsibilities of employees in organizations, just as rationalized bureaucratic organizations are expected to do to ensure efficiency and productivity.

4.1 Limitations

Our study is limited in several aspects. First, our study only interviewed enrolled students at one campus and majority of them were working in organizations or agencies in Hampton Roads area of Virginia, which make our findings will be limited in its generalizability. Second, this study did not ask about the participants' expectation for the on-the-job cybersecurity training program, including the appropriate delivery periodicity, the specific modules and skills, knowledges, and abilities that on-the-job cybersecurity training should prioritize and focus on. Previous study (Kam et al., 2022) indicates that situational interest together with situational motivational determinants such as perceived learning autonomy and perceived relatedness engendered self-determined motivation toward cybersecurity training. In addition, cybersecurity fatigue from cybersecurity training in workplace has been discussed (Reeves et al., 2021). Our study, however, is limited in probing further the respondents' expectations for cybersecurity training.

Even with the above-mentioned limitations, our study contributes to the current literature on cybersecurity training in workplaces by revealing the specific changes brought by the cybersecurity training program in employees' daily work behavior with employees' own words and experiences. Our study finds that providing on-the-job cybersecurity training is a bonus instead of a burden to organizations. Training and developing employees' cybersecurity awareness and technical skills is effective in improving the human capital for employees, the work team, and the organization, which will outweigh the investment costs by promoting productivity and maximizing profitability. On-the-job cybersecurity training is an effective human capital investment which provides valuable benefits to the individual employee as well as the employer. Organization's investment in training their employees to prevent cyberattacks and mitigate cybersecurity vulnerability in routine job environment positively contribute to improve the efficiency of the organization, the primary business goal for organization.

Acknowledgments

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This study was supported by the National Science Foundation, NSF #1956428. Yuying Shen contributed to designing the study, analyzing data, writing the manuscript, and revising the paper. Carlene Turner contributed to collecting data and analyzing data. Claude Turner contributed to literature review, and paper revision.

References

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69,* 437-443. https://doi.org/10.1016/j.chb.2016.12.040

Bhandari, M. P. (2020). Theories and Contemporary Development of Organizational Perspectives in Social Sciences. The founding writers of Western sociology. Part 1. *Scientific Journal of Bielsko-Biala School of Finance and Law*, *24*(1), 8-13. https://doi.org/10.5604/01.3001.0014.1342

Boddy, D. (1996). Information technology and organizational change. In *Information Management: The Organizational Dimension* (pp. 337-346). Oxford: Oxford University Press.

Brooks, C. (2022). Cybersecurity in 2022 -- A fresh look at some very alarming stats. *Forbes*. Retrieved from Jan.

21, 2022. https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Congressional Research Service Documents, CRS RL32331 (Washington DC), 2.

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis.* New York, NY: Sage Publications.

Corradini, I. (2020). *Building a Cybersecurity Culture in Organizations* (Vol. 284). Berlin/Heidelberg, Germany: Springer International Publishing. https://doi.org/10.1007/978-3-030-43999-6

Crumpler, W., & Lewis, J. A. (2019). *The Cybersecurity Workforce Gap.* Washington, DC, USA: Center for Strategic and International Studies (CSIS).

Gulick, L. (1937). Notes on the theory of organization. *Classics of Organization Theory*, *3*, 87-95. New York, NY: Routledge.

Hanushek, E. A., Ruhose, J., & Woessmann, L. (2015). Human capital quality and aggregate income differences: Development accounting for US states. CESifo Working Paper Series No. 5411. http://dx.doi.org/10.2139/ssrn.2627076

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249-257. https://doi.org/10.1080/10919392.2019.1611528

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2020). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, *21*(2), 203-213. https://doi.org/10.1108/JIC-05-2019-0112

Hirshfield, L., Bobko, P., Barelka, A. J., Costa, M. R, & Knott, B. A. (2015). The role of human operators' suspicion in the detection of cyberattacks. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *5*(3), 28-44. https://doi.org/10.4018/ijcwt.2015070103

Huang, K., & Pearlson, K. (2019). For what technology can't fix: Building a model of organizational cybersecurity culture. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 6398-6407). https://doi.org/10.24251/hicss.2019.769

IBM Security. (2021). *Cost of a Data Breach Report 2021*. Armonk: NY.

Jones, K. S., Namin, A. S., & Armstrong, M. E. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education (TOCE)*, *18*(3), 1-12. https://doi.org/10.1145/3152893

Kam, H. J., Ormond, D. K., Menard, P., & Crossler, R. E. (2022). That's interesting: An examination of interest theory and self-determination in organizational cybersecurity training. *Information Systems Journal*, *32*(4), 888-926. https://doi.org/10.1111/isj.12374.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: an empirical evidence. *Information Systems Frontiers*, *23*(2), 361-373. https://doi.org/10.1007/s10796-019-09977-z

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Livingston, J. (2021). What OSHA can teach us about cybersecurity: Many of the lessons and changes applied to manufacturing after the Occupational Safety and Health Act of 1970 can be applied to the growing challenge manufacturers face with industrial cybersecurity. Three keys to improving cybersecurity are highlighted. *Control Engineering*, *68*(2), 34-36. https://www.controleng.com/articles/what-osha-can-teach-us-about-cybersecurity/

Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review*, *14*(2), 5-10.

Mühlemann, S. (2016). *The Cost and Benefits of Work-Based Learning*. *OECD Education Working Papers,* 143. https://doi.org/10.1787/5jlpl4s6g0zv-en

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, *9*(3), 71-88. https://doi.org/10.2478/hjbpa-2018-0024

Oce, G. A. (2013). Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges. GAO-13-462T. Washington, DC.

Pasban, M., & Nojedeh, S. H. (2016). A Review of the Role of Human Capital in the Organization. *Procedia-Social and Behavioral Sciences*, *230,* 249-253. https://doi.org/10.1016/j.sbspro.2016.09.032

Reeves, A., Delfabbro, P., & Calic, D. (2021). Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. *SAGE open*, *11*(1). https://doi.org/10.1177/21582440211000049

Ritzer, G. (2013). *The McDonaldization of society*. Los Angeles, CA: SAGE Publications.

Rivera, L. (2020). Employer Decision Making. *Annual Review of Sociology*, *46*(1), 215-232. https://doi.org/10.1146/annurev-soc-121919-054633

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2021). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. In *Research Anthology on Artificial Intelligence Applications in Security* (pp. 174-188). IGI Global. https://doi.org/10.4018/978-1-7998-7705-9.ch008

Schultz, E. (2005). The human factor in security. *Computers & Security*, *24*, 425-426. https://doi.org/10.1016/j.cose.2005.07.002

Silverman, D. (2006). *Interpreting Qualitative Data: Methods for Analyzing Talk, Text, and Interaction*. Thousand Oaks, CA: Sage Publications.

Smith, A. (1776). *An Inquiry into the Nature and Causes of the Wealth of Nations*: Volume one. London: printed for W. Strahan and T. Cadell, 1776.

Sweetland, S. (1996). Human capital theory: Foundations of a field of inquiry. *Review of Educational Research*, *66*(3), 341-359. https://doi.org/10.3102/00346543066003341

Teixeira, P. N. (2007). Dr Smith and the moderns: Adam Smith and the development of human capital theory. In *The Adam Smith Review. (*Vol. 3, pp. 151-170). New York, NY: Routledge.

Tommey, C. R. (2018). Implications of Implementing Software Defined Networking to Improve Cybersecurity for Operational Technology Networks (Doctoral dissertation, Utica College).

Tsang, Mun C. (1997). The cost of vocational training. *International Journal of Manpower*, *18*(1/2), 63-89. https://doi.org/10.1108/01437729710169292

van Zadelhoff, M. (2016). The biggest cybersecurity threats are inside your company. *Harvard Business Review*, *19*.

Vieane, A., Funke, G., Gutzwiller, R., Mancuso, V., Sawyer, B., & Wickens, C. (2016). Addressing human factors gaps in cyber defense. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 60, No. 1, pp. 770-773). Los Angeles, CA: SAGE Publications. https://doi.org/10.1177/1541931213601176

Weber, M. (2009). *The Theory of Social & Economic Organization*. New York, NY: Simon and Schuster.

Zhang, Z., He, W., Li, W., and Abdous, M. (2021), Cybersecurity awareness training programs: a cost–benefit analysis framework, *Industrial Management & Data Systems*, *121*(3), 613-636. https://doi.org/10.1108/imds-08-2020-0462