Application of the Nudge Theory for Improving Information Security Awareness Campaigns

Abstract

Awareness campaigns play a crucial role in the implementation of information security management systems in any organization. A lack of sufficient awareness of information security threats among stakeholders has allowed many security breaches to occur, resulting in substantial financial and productivity losses. Information security awareness campaigns are traditionally created without much thought as to how users perceive them and whether they induce behavioral changes.[1] Research in behavioral economics has produced a better understanding of how external stimuli influence behaviors. The nudge theory, proposed in 2008, was a significant development in behavioral economics.[2]

The study that serves as the basis of this report analyzes the impact of using the nudge theory to create information security awareness posters containing nudges, with the ultimate goal of improving their effectiveness. An online focus group of 51 working professionals who participated in a web-based survey was used to conduct the study. Data collected from the focus group survey found that nudge-based posters resulted in positive behavior changes in viewers. The data were analyzed using the weighted sum model, which determined that the weighted sum score of a nudge-based poster containing a discouraging nudge was 11 percent higher than the non-nudge poster. Study findings provide strong evidence for the applicability of the nudge theory in improving the effectiveness of information security awareness posters.

Introduction

Increased integration of people, processes and technology has become an essential requirement for tackling the modern cybersecurity landscape.[3] Organizations worldwide were forced to accept new normal working conditions due to the COVID-19 pandemic in early 2020. The world is witnessing the adoption of new working models such as work from home (WFH), shifting enterprise information repositories to cloud-based storage and using collaborative tools for seamless remote work. Some organizations had already put many such activities into practice before the pandemic as a result of the growth of the gig economy.[4]

In 2020, more than 40 percent of the threat actors behind confirmed data breaches were outsiders, including organized criminal groups and hacktivists.[5] The rise of attacks by hacktivists is an emerging trend that governments and organizations must address. Risk created by employees contributed to around 20 percent of the confirmed breaches, which is also a concern for information security managers.[6] An increase in public cybersecurity awareness campaigns as a capacity-building measure has been noted.[7] However, the percentage of cybersecurity educational programs and other training efforts specifically for professionals in the countries that participated in the survey is relatively low. Only 46 percent of countries reported providing nation-

SUDEEP SUBRAMANIAN | PH.D., CISA, SMACM

Is an associate professor in the area of international business at FORE School of Management (New Delhi, India). He has more than 18 years of experience in the IT and management education domain. His IT industry experience includes software development, project management, information systems audit and information security consulting.

The heightened prominence of information security awareness training among organizations and governments has propelled new research in academia and encouraged practitioners to find better ways to develop…information security awareness programs.

specific training to government or public sector employees, and 41 percent of private or small and medium-sized enterprises (SMEs) provided capacity-building training.[8] There is a considerable shortfall in initiatives for providing cybersecurity awareness campaigns.

A recent study conducted among Danish organizations reported that implementation of awareness training and cyberhygiene procedures was found to be 48 percent and 43 percent, respectively.[9] Such a low level of implementation of information and cybersecurity improvements is cause for concern, as 77 percent of respondents felt that the perceived threat level against their organization had increased.[10]

There have been calls for drastic changes to the way security awareness training is designed and delivered.[11] Researchers have argued that security awareness training should move beyond traditional check-the-box compliance. Instead, awareness training should be taken to the next level with the aim of creating training programs that capture the workforce's attention with better communication retention levels. Organizations should halt traditional approaches and security specialists should develop new and creative ideas. Information security-related risk does not merely affect organizations—it has global implications.

Many countries are now offering electronic versions of government-to-citizen (G2C) services, and citizens must have sufficient awareness about the information security risk inherent in G2C or business-to-consumer (B2C) services. Therefore, many national governments are now prioritizing proper information security awareness training for their citizens.

One such initiative was spawned by the European Union Agency for Cybersecurity (ENISA), which conducted a feasibility study in 2011 on providing information security training programs or events.[12] ENISA designated European Cybersecurity Month (ECSM) as a security awareness training program targeted to groups such as citizens, officials working in government, private organizations, and other target groups that require specialized training programs. The purpose of this initiative was to develop holistic, annual events designed to raise awareness of information security. The feasibility study for ESCM involved the creation of a road map for rolling out the program among member countries. The road map contained a detailed discussion of how to make the program interesting and the topics on which security awareness campaigns could be developed. The ECSM was launched in 2012 with activities to be conducted on an annual basis. The last ECSM took place in October 2020; it consisted of 419 activities (a decrease of 22 percent due to the COVID-19 pandemic), and approximately 9.8 million users viewed ECSM content.[13]

It should be noted that campaigns such as ECSM are required to improve the cyberhygiene of all stakeholders. In 2017, ENISA released a report on cyberhygiene practices followed in private and government establishments in Europe.[14] The cyberhygiene report contained a detailed overview of the leading European cyberhygiene programs and included recommendations for improving cyberhygiene in Europe. One key recommendation was improving the cybersecurity awareness programs in organizations, particularly SMEs that lacked the necessary resources and personnel to implement satisfactory security management systems.

The heightened prominence of information security awareness training among organizations and governments has propelled new research in academia and encouraged practitioners to find better ways to develop more robust and efficient information security awareness programs. Information security specialists should explore new ways of designing, developing and administering awareness programs to ensure better outcomes.

An emerging category of information security research is behavioral information security research, which focuses on studying aspects of insider misbehavior, actions of hackers, improvement of information security compliance and cross-cultural behavioral information security.[15] An exploratory

study was conducted across three Australian organizations to determine practical ways to build a security culture to change employee behavior. The study proposed five key initiatives, which included alignment between internal and external campaigns to transform security awareness from compliance to culture.[16]

Similarly, an experimental study was conducted in which respondents were presented with personalized security warning messages for browsers using the nudge theory's choice architecture approach.[17] Although study results did not provide any evidence that personalized nudge messages resulted in intended behavior changes, they offered valuable insights for future research in this direction. In an online experiment conducted by researchers from the EU's Joint Research Centre (JRC), it was found that warning messages shown in the form of nudges generated more secure online behavior in users accessing a mock online storefront.[18]

> Employees should be constantly reminded about the importance of complying with information security rules and regulations.

Based on the aforementioned research conducted to identify ways to improve cybersecurity awareness programs, this study includes an attempt to determine whether nudges can be incorporated in information security awareness posters to improve compliance with the posters' messages. Posters are an important medium used for the communication of security awareness messages. Governments and private enterprises use information security awareness posters to convey critical awareness-related messages to targeted users. The design of information security awareness posters typically follows a traditional approach, using an image, text or a combination of both to convey the message.

In an *ISACA® Journal* article, researchers discussed the nudge theory and examples of nudges applied in various business and social contexts.[19] A flowchart for creating a nudge-based security awareness poster was developed and two nudge-based posters were created. In the study outlined herein, researchers discuss the finding of an earlier study conducted among professionals working in different enterprise sectors to determine whether nudge and non-nudge posters made any difference in information security behavior.

Problem Statement

Enterprises handle sensitive client information and rely heavily on their information systems for day-to-day operations. Information systems assets are constantly under threat from external and internal actors who may launch cyberattacks at any time. Worldwide spending on information security (a segment of the broader cybersecurity market) reached US$114 billion in 2018, an increase of 12.4 percent from 2017. An increase in demand from US$124 billion in 2019 to US$170.4 billion in 2022 is expected.[20]

To combat cyberthreats, organizations are launching information security programs to motivate employees to comply with information security policies. Organizations are also investing their capital and time on induction programs, online modules and audits, but many employees are still not motivated to follow all the rules and regulations. There has been no shortage of data breach reports due to cyberattacks from internal or external sources (**figure 1**).

To prevent cyberattacks caused by insiders, intentionally or unintentionally, organizations must motivate their employees and make them aware of potential cybersecurity risk areas. Employees should be constantly reminded about the importance of complying with information security rules and regulations. The problem query for this study is "How can information security awareness programs be improved to increase compliance from all stakeholders?"

Study Objectives

The main objectives of this study are:

1. To analyze the results of using the nudge theory to motivate behavioral changes toward security compliance by employees
2. To create information security posters using the nudge theory
3. To assess the impact of nudge-based posters among employees

FIGURE 1

Security Breach Incidents

Organization	Cyberattack	Details
Waymo (Google's self-driving car project)[a]	An insider stole confidential data and provided them to a competitor.	Anthony Levandowski, Waymo's lead engineer, left to found a start-up called Otto that developed self-driving trucks. Uber acquired Otto in several months, and Levandowski was put in charge of Uber's self-driving department. Levandowski stole trade secrets from Google and provided them to Uber.
Launch Point (an insurance coordination services vendor)[b]	In 2017, a data breach was executed by an employee who emailed a file containing protected health information (PHI) to his private email address.	The file included US Medicare ID numbers, contract numbers, health plan ID numbers, the dates of enrollment of 18,580 customers and some customers' last names and dates of birth. Launch Point contacted these individuals and provided them with two years of free credit monitoring and identity theft restoration services.
Dubsmash (New York, USA-based video messaging service)[c]	In December 2018, data were stolen and listed for sale on the dark web's Dream Market.	Data included 162 million email addresses, usernames, PBKDF2 password hashes and other personal data such as dates of birth. Dubsmash failed to disclose how the attackers got in or how many users were affected.
Cognizant Technology Solutions Corp[d]	In April 2020, Cognizant was hit by a Maze ransomware cyberattack, resulting in service disruptions for some clients.	The Maze operators denied responsibility for the cyberattack. The ransomware attack resulted in the encrypting of user data files and the attackers demanded a hefty sum to restore the files to their original state.

Sources: a) EKRAN, "Five Real-Life Examples of Breaches Caused by Insider Threats," 18 November 2020, *https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches*; b) *Ibid*. c) Hill, M.; D. Swinhoe; "The 15 Biggest Data Breaches of the 21st Century," *CSO*, 16 July 2021, *https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.amp.html*; d) Reuters, "Cognizant Hit by 'Maze' Ransomware Attack," 18 April 2020, *https://www.reuters.com/article/us-cognizant-tech-cyber-idUSKBN2200YA*

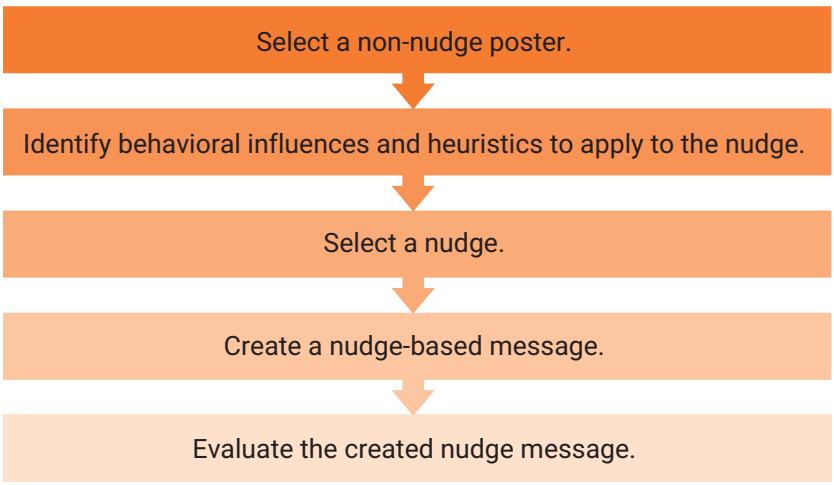
Research Propositions

The following research propositions (RPs) were formulated to achieve the research objectives:

- **RP1**—Nudge theory can be used for behavioral changes among employees for better information security compliance.
- **RP2**—Nudge-based information security posters in organizations have a positive impact on information security compliance among employees.
- **RP3**—There is a difference between how male and female respondents perceive nudge and non-nudge posters.

FIGURE 2

Flowchart for Nudge Poster Conversion



Research Design

Researchers introduced libertarian paternalism as part of an emerging branch of behavioral economics, which is a marriage between economic theories and experimental methods psychology.[21] According to libertarian paternalism, providing a choice architecture that alters the user's behavior is fair if the end results are to the advantage of the user. The presentation of choice architecture as a nudge is done in a noncoercive manner and does not forbid users to make alternate choices.[22] Nudge theory, which originated in behavioral economics, has been applied in many scenarios, such as increasing voter turnout in elections, reducing littering, increasing savings participation and increasing participation in water conservation.

Nudges can be designed with four dimensions in mind:

1. Boosting self-control vs. activating the desired behavior
2. Externally imposed vs. self-imposed
3. Mindful vs. mindless
4. Encouraging vs. discouraging[23]

In the study discussed herein, a flowchart for converting a non-nudge poster into a nudge-based poster was developed using the approaches of previous studies (**figure 2**).[24]

Select a Non-Nudge Message

A suitable non-nudge poster must be selected for conversion and, in this study, the non-nudge poster provided tips for keeping passwords safe (**figure 3**). Raising awareness about password management and the importance of setting high-security passwords is the main goal of many information security awareness campaigns.

Identify Behavioral Influences and Heuristics to Apply the Nudge

Most password management campaigns focus on providing specific rules that should be kept in mind when setting a password. One drawback of this approach is the effectiveness of these campaigns—or lack thereof. It has been noted that many users find these messages repetitive and do not take them seriously.[25] Thus, users experience information overload and confirmation bias when deciding to take action based on a campaign message. However, there is a possibility for a behavioral change to occur if employees are made aware of the security risk associated with choosing a weak password. Another behavioral influence could result from educating employees about the potential financial losses related to misuse of passwords by hackers (i.e., loss aversion).

Based on the identified behavioral influences, the heuristics to apply the nudge should be formulated. The heuristics chosen to improve password management are anchoring and adjustment, and social proof.[26] Anchoring and adjustment are suitable in this context because the anchor can provide a reference to the user. Based on the anchor, the user may be nudged to make a behavior change. Social proof is widely used as it demonstrates to users the behavioral patterns of their peers. The probability of users trying to adapt their behavioral patterns to conform to social norms is high.

FIGURE 3

Non-Nudge Poster 1

Source: Adapted from McAfee, "Fifteen Tips To Better Password Security," June 2011, *https://www.mcafee.com/blogs/internet-security/15-tips-to-better-password-security/*

Select a Nudge

Researchers developed two posters using different nudge dimensions based on behavioral influences and heuristics analyzed for the selected non-nudge poster. The first poster was designed with a combination of the following nudge dimensions: externally imposed, mindful and discouraging with

FIGURE 4

Discouraging Nudge Poster 2

Source: Adapted from Verizon, *2017 Data Breach Investigation Report 10th Edition*," USA. 2017, *https://www.verizon.com/business/resources/reports/2017_dbir.pdf*

If the nudge-based poster does not produce the intended behavioral change, a thorough review must be performed to analyze the reasons for failure and explore the possibilities of revising the poster to make it more effective.

the desired user behavior of adoption of a stronger password. The second poster was designed with the following nudge dimensions: externally imposed, mindful and encouraging. Therefore, the two posters aim to elicit positive user behavior in two ways. The first poster aims to alert the user with a negative message and discourages using a weak password. The second poster aims to inform the user with a positive message and thus encourages the user to adopt that behavior.

Create the Nudge-Based Poster

The first poster containing a nudge with a discouraging message was developed by displaying findings of a data breach report released by Verizon (**figure 4**).[27] The alarming statistic of how many data breaches were reported due to weak password usage is the discouraging nudge message. The second poster, which contains an encouraging nudge, was designed to display information about positive social behavior of strong password adoption among the organization's users and encourage viewers to join that community of users (**figure 5**). The intended user behavior was to motivate users in a positive manner to adopt stronger passwords.

FIGURE 5

Encouraging Nudge Poster 3

Evaluate the Effectiveness of the Nudge-Based Poster

The evaluation of the effectiveness of the nudge-based poster is a crucial phase in the flowchart for nudge conversion. If the nudge-based poster does not produce the intended behavioral change, a thorough review must be performed to analyze the reasons for failure and explore the possibilities of revising the poster to make it more effective. An ineffective poster could be the result of an error in judging the behavior influences and identifying the heuristics used while designing a nudge. The creation of the poster also may contain lacunae in the form of inadequately framing the nudge message or failing to create a poster that catches target viewers' attention. Such errors can be identified and corrected if a proper evaluation of the nudge poster is carried out in a systematic manner.

Many different approaches were used in previous studies to measure the effectiveness of advertisement campaigns, branding and similar marketing communications.[28, 29, 30] Most of the studies used marketing theories to develop a methodology for measuring marketing communication effectiveness. They used qualitative or quantitative techniques to analyze study findings. In this study, to measure the effectiveness of the poster and determine whether it produced the desired user behavioral change, a theory of communication called the Attention, Interest, Desire and Action (AIDA) model was selected.

The AIDA model can be used to measure the cognitive process an individual goes through while receiving a new idea or message, and the action taken by the individual based on the message received.[31] Using the AIDA model as a reference, a set of questions was drafted and administered to individuals after they were shown the three posters (**figure 6**). The questions were prepared using each of the elements of the AIDA model, and quantitative responses in the form of a rating and qualitative responses in the form of a typed answer were collected.

FIGURE 6

Questionnaire for the Discouraging Nudge Poster

Please respond to the following questions:

1) How do you rate this poster on its attractiveness?
   Your rating (1–10, 1 = Least attractive, 10 = Most attractive) : ____
   Please give your reasons/comments on the rating given :

2) How do you rate this poster on its ability to generate interest in password management?
   Your rating (1–10, 1 = Least interested, 10 = Most interested) : ____
   Please give your reasons/comments on the rating given :

3) How do you rate this poster on its ability to generate the desire to improve password management?
   Your rating (1–10, 1 = Least desired, 10 = Most desired) : ____
   Please give your reasons/comments on the rating given :

4) Are you planning to change your current password to a stronger one after viewing this poster?
   Your rating (1–10, 1 = No change planned , 10 = Definitely going to change) : ____
   Please give your reasons/comments on the rating given :

Research Method

The required data for the study were collected using the focus group method. The focus group method involves a study that is conducted by inviting 8-10 respondents and conducting detailed interviews using open-ended questions about the topic being researched.[32] The researcher plays the role of a moderator and tries to elicit the required information from the participants. Traditionally, focus groups are conducted face-to-face, but in case of barriers to conducting the study in a physical setting, they also be conducted electronically. One may conduct online focus groups in a synchronous mode, in which the researcher conducts a live discussion with the participants using electronic communication aids, or in an asynchronous mode, in which the researcher collects data for the study by hosting a questionnaire on a website or disseminating a prepared questionnaire through emails or online forums.[33]

This study was conducted during the national lockdown period in India from April–May 2020. At that time, there were restrictions on conducting physical meetings with participants in person. Therefore, the researchers conducted the study using the online focus group method in the asynchronous mode. Fifty participants from India were chosen to respond, representing a balanced gender mix, employment in diverse business sectors and a combination of experience levels.

A questionnaire containing both closed and open-ended questions was developed and distributed as a Google Form survey. The questionnaire contained four sections: Section 1 was used to collect the participant's demographic information (**figure 7**), and sections 2, 3 and 4 contained three posters used for the study. A simple multicriteria decision analysis technique and weighted sum model were used to analyze the ratings given by the participants. The weighted sum model can be used to select the best alternative from multiple choices, which must be rated using different criteria and weights.[34]

In this study, the choice alternatives that were evaluated were the three posters, and the criteria used were the elements of the AIDA model. The application of the weighted sum model resulted in four criteria, and an equal weight of 0.25 was applied while calculating the weighted sum for each poster. The responses collected through the open-ended questions were analyzed using thematic analysis. Thematic analysis is used in qualitative research to identify themes related to the study topic within participants' responses.[35]

FIGURE 7

Participant Demographics Questionnaire

Questions	Response Options
Gender of respondent?	Male/Female/Other
Age of respondent (in years)?	Younger than 20 21–30 31–40 41–50 Older than 50
Sector of organization?	Banking IT industry Manufacturing Consulting Other
Position in organization?	Junior level Middle level Senior level
Years of experience?	Less than 2 years 2–5 years 5–10 years More than 10 years
Information security management system in place within the organization?	Yes No In planning stage Final stage of implementation
Is the organization certified in ISO 27001?	Yes No In planning stage Final stage of implementation Do not know

Results

The demographic characteristics of participants of the online focus group survey were collected (**figure 8**). The key demographic indicators include the gender mix of 61 percent male and 39 percent female out of 51 participants. It was noted that 92 percent of the participants were in the age group of 21 to 30 years. The participants were predominantly from the IT industry (78 percent), and the majority held mid-level positions (55 percent) in their organizations.

One crucial characteristic that had a positive influence on the study is that 76 percent of the participants were employed in an organization that was International Organization for Standardization (ISO) 27001-certified. An employee of an ISO 27001-certified organization may have previously attended information security training programs or been exposed to information security awareness posters in electronic and print formats.

Discussion of Analysis of Poster Ratings

The ratings given by each participant on a scale of 1 to 10 for each element of the AIDA model were analyzed for the three posters. When the average score for the four elements of the AIDA model was computed, Poster 2 scored the highest average rating across all four elements.

Poster 2, which contains a nudge based on a discouraging message of data breach reporting, earned the highest score for the attention, interest, desire and action steps in the AIDA model. This finding indicates that Poster 2 was able to capture the attention of the viewer; it generated an interest in password security; it created a desire to adopt a better password generation scheme; and it inspired the viewer to perform an action based on the poster message. The ratings of Poster 3, a poster designed with an encouraging nudge, came in the second position in terms of the average ratings for each

FIGURE 8

Demographic Characteristics

Demographic Characteristics		Count/Percent
Gender	Male Female Other	31 (61 percent) 20 (39 percent) 0
Age	Younger than 20 21–30 31–40 41–50 Older than 50	0 47 (92 percent) 2 (4 percent) 1 (2 percent) 1 (2 percent)
Sector of organization	Banking IT industry Manufacturing Consulting Other	2 (4 percent) 40 (78 percent) 1 (2 percent) 2 (4 percent) 6 (12 percent)
Position in organization	Junior level Middle level Senior level	19 (37 percent) 28 (55 percent) 4 (8 percent)
Years of experience	Less than 2 2–5 5–10 More than 10	12 (23 percent) 33 (65 percent) 2 (4 percent) 4 (8 percent)
Information security management system in the organization	Yes No In planning stage Final stage of implementation	49 (96 percent) 1 (2 percent) 1 (2 percent) 0
Is organization ISO 27001-certified?	Yes No In planning stage Final stage of implementation Do not know	39 (76 percent) 2 (4 percent) 1 (2 percent) 0 9 (18 percent)

element of the AIDA model. Thus, Poster 2 and Poster 3, nudge-based posters, performed better than the non-nudge Poster 1 in the study (**figure 9**).

The cumulative effect of all the steps in the AIDA model was analyzed by computing and averaging the weighted sum for each respondent (**figure 10**). The average weighted sum for Poster 2 was the highest among all the posters, followed by Poster 3. If the average weighted sum score of Poster 1 is considered the baseline, then the weighted sum score of Poster 2 is 11 percent, and Poster 3 is 6.85 percent higher than Poster 1. Per these findings, one can conclude that Poster 2 and Poster 3 were more effective than Poster 1 based on the responses of the study participants.

The average weighted sum for each poster was computed separately to analyze if any difference in perception existed between the female and male respondents (**figure 11**). Average ratings given by females were significantly higher than those of males. The weighted sum score for Poster 2 for female respondents was 8.5, and for males was 7.87. The

FIGURE 9

Average Ratings for All Posters

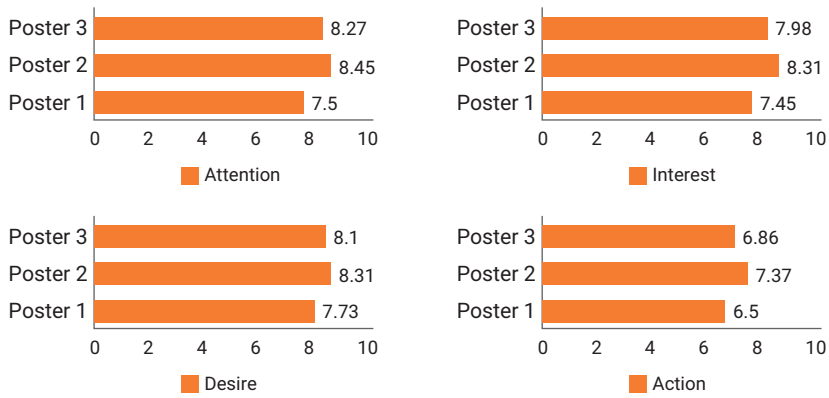
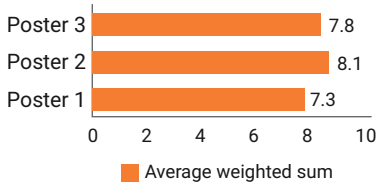


FIGURE 10

Average Weighted Sum for All Posters



weighted sum score is higher than the cumulative score for females and males, which is 8.1. This finding suggests that the information security awareness campaign was perceived differently by females and males.

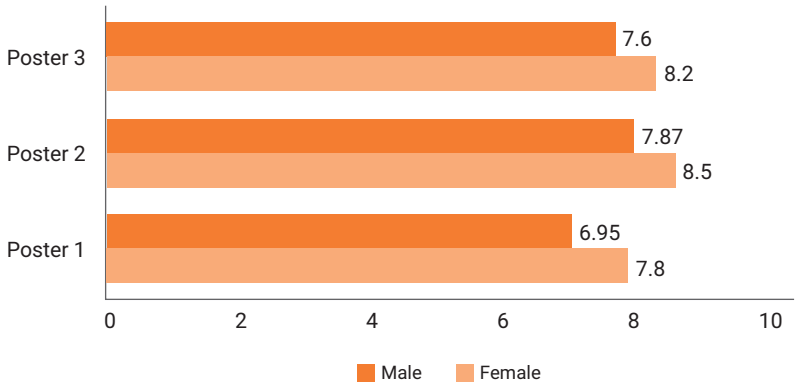
Implications

The findings of this study present new opportunities for research in improving the design of information security awareness campaigns. Research in information security is a relatively new field of study with a short span of existence. However, with the increase in digital transformation in organizations and governments, research into improving information security awareness and evaluating the improvements is gaining the attention of stakeholders across the board.

This study provides a model for improving information security poster design using the nudge theory as the theoretical framework. Though a relatively new theory in behavioral economics, the nudge theory has been used extensively in various business use cases with positive results. This study provides evidence of the applicability of the nudge theory in the context of information security compliance. For practitioners, this study offers an opportunity to rethink strategies for information security awareness campaigns. The findings of this study present a case for benefits for improving enterprise information security awareness campaigns.

FIGURE 11

Average Weighted Sums of Male and Female Respondents



Limitations

This study was conducted using a multicriteria decision technique, and its findings have not been statistically tested. Therefore, the findings cannot be generalized. The use of the online focus group method does have many positive characteristics. Still, the main drawback of this method is the lack of face-to-face interaction between the researchers and respondents. This lack of personal interaction does present certain challenges, particularly in the collection of qualitative data. The current study suffers a drawback concerning the collection of data.

Future Scope

The findings of the study present opportunities for future studies in this area. As the world becomes increasingly digitalized, the importance of information security research and, more specifically, research into behavioral aspects concerned with improving information security awareness effectiveness cannot be understated. Researchers may develop future studies by building theoretical models and testing hypotheses. Data collected from such studies may be analyzed using quantitative statistical techniques that may yield statistically tested results. Researchers may conduct future studies using the nudge theory or similar theories to improve information security awareness campaigns.

Conclusion

Managing information security in an organization is a complex task, and any lapses in efficient management can lead to catastrophic consequences. Information security managers in any organization constantly strive to implement more effective information security management systems to counter emerging cybersecurity challenges.

A critical aspect of information security management that has not been addressed adequately is the management of information security awareness campaign design and implementation. This study was developed to address this gap in information security research. The main objective of this study was to analyze whether the nudge theory can be used to

create information security awareness posters that are more effective than traditional awareness posters. As a part of this study, three research propositions were framed and the research study was planned, including use of the online focus group method.

The analysis of the data collected provided positive evidence for acceptance of all research propositions framed. Therefore, analysis of the study findings proved that the nudge theory could be used for behavioral changes among employees for better information security compliance (RP1), nudge-based posters had a positive impact on information security compliance among employees (RP2), and there was a measurable difference between female and male respondents' perception of the nudge-based posters (RP3).

These study findings provide helpful pointers for further research on applying the nudge theory for improving information security compliance. Still, this research area is in its nascent stage. Future studies in this domain may pave the way to building better information security awareness campaigns.

A critical aspect of information security management that has not been addressed adequately is the management of information security awareness campaign design and implementation.

Author's Note

The infrastructural support provided by the FORE School of Management (New Delhi, India) is gratefully appreciated. This study is derived from an academic project created by Udita Agrawal, a student, under the guidance of Sudeep Subramanian, Ph.D. The author gratefully acknowledges the support from Udita Agrawal in the successful completion of this study.

Endnotes

1 Opacki, J.; "Building a Security Culture: Why Security Awareness Does Not Work and What to Do Instead," *ISACA® Journal*, vol. 5, 2017, *https://www.isaca.org/archives*
2 Thaler, R. H.; C. R. Sunstein; *Nudge: Improving Decisions About Health, Wealth, and Happiness, Revised and Expanded Edition*, Penguin Books, USA, 2009
3 Cosgrove, A.; "Cybersecurity in 2021: People, Process and Technology to Integrate More Than Ever Before," *Infosecurity Magazine*, 20 January 2021, *https://www.infosecurity-magazine.com/blogs/cybersecurity-2021-people-process/*
4 Kuhn, K. M.; "The Rise of the 'Gig Economy' and Implications for Understanding Work and Workers," *Industrial and Organizational Psychology*, vol. 9, iss. 1, March 2016, *https://www.cambridge.org/core/journals/industrial-and-organizational-psychology/article/abs/rise-of-the-gig-economy-and-implications-for-understanding-work-and-workers/0359098FEC51B66EFC02101105B25FCF*
5 Ernst & Young (EY), *EY Global Information Security Survey 2020,* United Kingdom, 2020, *https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-report.pdf*
6 *Ibid*.
7 The International Telecommunication Union (ITU), *Global Cybersecurity Index 2020*, Switzerland, 2021, *https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx*
8 *Ibid*.
9 Deloitte, *2020 Deloitte Cyber Survey*, United Kingdom, 2020, *https://www2.deloitte.com/content/dam/Deloitte/dk/Documents/Cyber/cyberreport/Cyber_survey_.pdf*
10 *Ibid*.
11 Haney, J.; W. Lutters; "Security Awareness Training for the Workforce: Moving Beyond 'Check-the-Box' Compliance," *Computer*, vol. 53, iss. 10, October 2020, *https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8201414/*
12 European Union Agency for Cybersecurity (ENISA), *European Month of Network and Information Security for All - A Feasibility Study*, Greece, 14 December 2011, *https://www.enisa.europa.eu/publications/europeansecuritymonth*
13 European Union Agency for Cybersecurity, *European Cybersecurity Month 2020—Deployment Report,* Greece, 15 April 2021, *https://www.enisa.europa.eu/publications/ecsm-deployment-report-2020*
14 European Union Agency for Cybersecurity, *Cyber Hygiene*, Greece, 17 February 2017, *https://www.enisa.europa.eu/publications/cyber-hygiene*

ENJOYING THIS ARTICLE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

15 Crossler, R. E.; A. C. Johnston; P. B. Lowry; Q. Hu; M. Warkentin; R. Baskerville; "Future Directions for Behavioral Information Security Research," *Computers and Security*, vol. 32, February 2013, *https://www.sciencedirect.com/science/article/pii/S0167404812001460?via%3Dihub*

16 Alshaikh, M.; "Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective," *Computers and Security*, vol. 98, November 2020, *https://www.sciencedirect.com/science/article/pii/S0167404820302765?via%3Dihub*

17 Malkin, N.; A. Mathur; M. Harbach; S. Egelman; "Personalized Security Messaging: Nudges for Compliance With Browser Warnings," EuroUSEC '17, 2017, *https://www.ndss-symposium.org/wp-content/uploads/2018/03/eurousec2017_08_Malkin_paper.pdf*

18 European Union Agency for Cybersecurity, *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, Greece, 12 April 2019, *https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity*

19 Subramanian, S.; U. Agrawal; "Nudging Our Way to Successful Information Security Awareness," *ISACA Journal*, vol. 1, 2021, *https://www.isaca.org/archives*

20 Morgan, S.; "Global Cyber Security Spending Predicted to Exceed $1 Trillion From 2017–2021," *Cybercrime Magazine*, 10 June 2019, *https://cybersecurityventures.com/cybersecurity-market-report/*

21 *Op cit* Thaler

22 Thaler, R. H., C. R. Sunstein, "Libertarian Paternalism," *American Economic Review*, vol. 93, iss. 2, May 2003, h*ttps://www.aeaweb.org/articles?id=10.1257/000282803321947001*

23 Ly, K.; N. Mazar; M. Zhao; D. Soman; "A Practitioner's Guide to Nudging," Rotman School of Management Working Paper No. 2609347, University of Toronto, Ontario, Canada, 15 March 2013, *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2609347*

24 Coventry, L.; P. Briggs; D. Jeske; A. van Moorsel; "SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment," *Lecture Notes in Computer Science*, vol. 8517, *https://link.springer.com/chapter/10.1007/978-3-319-07668-3_23*

25 Schneier, B.; "Security Design: Stop Trying to Fix the User," *IEEE Security and Privacy*, vol. 14, iss. 5, 25 October 2016, *https://ieeexplore.ieee.org/document/7676198*

26 Tversky, A.; D. Kahneman; "Judgment Under Uncertainty: Heuristics and Biases," *Science*, vol. 185, iss. 4157, 27 September 1974, *https://www.science.org/doi/10.1126/science.185.4157.1124*

27 Verizon, *2017 Data Breach Investigations Report*, *10th Edition,* USA, 2017, *https://www.verizon.com/business/resources/reports/2017_dbir.pdf*

28 Patsioura, F.; M. Vlachopoulou; V. Manthou; "A New Advertising Effectiveness Model for Corporate Advertising Web Sites," *Benchmarking: An International Journa*l, vol. 16, iss. 3, 2009, *https://www.academia.edu/1078104/A_new_advertising_effectiveness_model_for_corporate_advertising_web_sites_A_relationship_marketing_approach*

29 Reiser, A.; D. G. Simmons; "A Quasi-Experimental Method for Testing the Effectiveness of Ecolabel Promotion," *Journal of Sustainable Tourism*, vol. 13, iss. 6, 2005, *https://www.tandfonline.com/doi/abs/10.1080/09669580508668583*

30 Redmond, E. C.; C. J. Griffith; "A Pilot Study to Evaluate the Effectiveness of a Social Marketing-Based Consumer Food Safety Initiative Using Observation," *British Food Journal*, vol. 108, iss. 9, 1 September 2006, *https://www.researchgate.net/publication/240601672_A_pilot_study_to_evaluate_the_effectiveness_of_a_social_marketing-based_consumer_food_safety_initiative_using_observation*

31 Hassan, S.; S. Z. A. Nadzim; N. Shiratuddin; "Strategic Use of Social Media for Small Business Based on the AIDA Model," *Procedia Social and Behavioral Sciences*, vol. 172, 27 January 2015, *https://www.sciencedirect.com/science/article/pii/S1877042815004000?via%3Dihub*

32 Calder, B. J.; "Focus Groups and the Nature of Qualitative Marketing Research," *Journal of Marketing Research*, vol. 14, iss. 3, August 1977, *https://www.jstor.org/stable/3150774*

33 Rezabek, R.; "Online Focus Groups: Electronic Discussions for Research," *Forum: Qualitative Social Research*, vol. 1, 2000, *https://www.qualitative-research.net/index.php/fqs/article/view/1128/2509*

34 Triantaphyllou, E.; "Multi-Criteria Decision-Making Methods: A Comparative Study," *Applied Optimization*, vol. 44, 2000, *https://link.springer.com/chapter/10.1007/978-1-4757-3157-6_2*

35 Caelli, K.; L. Ray; J. Mill; "'Clear as Mud:' Toward Greater Clarity in Generic Qualitative Research," *International Journal of Qualitative Methods*, vol. 2, iss. 2, 2003, *https://journals.sagepub.com/doi/10.1177/160940690300200201*