Nudging Our Way to Successful Information Security Awareness

Ensuring the security of information flowing in an organization requires the attention of all stakeholders including top management, employees and customers. Compliance with information security policies should be taken seriously with small or large organizations to avoid security risk, data breaches, or any attack on information and software. To achieve this goal, employee understanding of information security issues should be improved through training programs.

Despite organizations' initiatives and awareness programs, employees can be reluctant to follow all the rules and regulations in place to maintain information security. Employees often complete actions that are not compliant with information security policies such as sharing passwords, using social media websites on organization devices and leaving project-related notes unattended. The lack of information security compliance among employees leads to many security breaches and loss of data. To avoid these kinds of threats, organizations should focus more on security policies and getting all employees to comply with them.

Along with strengthening the security strategy, organizations need to manage those employees and stakeholders who do not follow them and, therefore, create security threats. However, if organizations follow a highly restrictive security policy, it will limit the flexibility of employees, which might result in resentment among employees. A 2017 *ISACA®* *Journal* article noted gaps in information security awareness training and observed whether the training serves its purpose of mitigating security threats due to attacks such as phishing.[1] The article discussed the need to create a "culture of security" in organizations that goes beyond the traditional security awareness training and mechanisms for tracking its improvement. In a study conducted by Quagliata, it was observed that organizations could employ multiple training methods that include various tools such as posters, newsletters and brochures to improve the perceived security effectiveness.[2]

The human aspects of cybersecurity are essential factors that have not been considered by both researchers and practitioners. In 2018, the European Union Agency for Network and Information Security (ENISA) published a report

Sudeep Subramanian, Ph.D., CISA, SMACM
Is an associate professor of international business at FORE School of Management (New Delhi, India). He has 17 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.

Udita Agrawal
Is a postgraduate student specializing in international business and marketing at the FORE School of Management. She has worked as a software developer at Tata Consultancy Services.

> A NUDGE IS A BEHAVIORAL SCIENCE CONCEPT THAT ALTERS PEOPLE'S BEHAVIOR IN A PREDICTABLE WAY WITHOUT FORBIDDING ANY OPTIONS OR SIGNIFICANTLY CHANGING THEIR ECONOMIC INCENTIVES.

which discussed the need for building a cybersecurity culture framework in organizations.[3] Cybersecurity culture can be defined as the norms, beliefs, perceptions, attitudes and assumptions of people regarding cybersecurity. The implementation of cybersecurity culture calls for the application of tools and techniques that are successful in other fields such as psychology, behavioral sciences, human factors and economics.[4] One approach for improving information security awareness, which is a constituent of the cybersecurity culture framework, is to apply the nudge theory, a behavioral economics theory. Nudge theory involves the use of introducing behavioral changes in people by altering the choice architectures.[5] Nudge theory can be used to create behavioral changes among employees without forcing or pressuring them to follow all security rules, instead by motivating them and altering their decisions and habits to maintain all security policies.

Nudge Theory and Its Applications

A nudge is a behavioral science concept that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To be counted as a mere nudge, the intervention must be cheap and easy to avoid. Nudges are not mandates; they are indirect suggestions to influence the behavior and decision-making of an individual.[6] The nudge theory relies on the philosophy of "libertarian paternalism."[7] Even though both libertarianism and paternalism are opposing moral principles, it is argued that providing guidance to people when choosing the best alternative from a set of choices for overall community welfare is beneficial to all stakeholders.

The concept of presenting a "choice architecture" as a "nudge" can be explained using an example.[8] Assume that two school cafeterias are trying to reduce the consumption of junk food among children, and they each adopted a different mechanism to do it. The first cafeteria attacks the problem by banning the sale of junk food. The other cafeteria changes the display of food items by shifting junk food to a higher shelf that is hard for children to reach and placing healthier food items at eye level where they are easily visible and approachable. Both cafeterias used two very different approaches to try to control the consumer's actions. The first cafeteria influences actions by limiting choices, and, thus, the consumer's complete freedom of choice. But the second cafeteria uses a nudging technique—altering the choice architecture to draw attention away from the junk food, thereby increasing the probability of healthier items being selected by the consumer. When using a nudge, it is important to note that behavior is not influenced by restrictions or adding any economic incentives, rather it is influenced by changing the presentation of the choices.

When devising a framework for designing nudges, it can be classified into four dimensions:[9]

1. **Boosting self-control vs. activating a desired behavior**—Nudges that are designed to boost self-control are used to influence individuals to make a decision that they think might be beneficial to them in the long run but that they might not be interested in at that particular time. A good example of this class of nudge is contributing to a retirement fund early in employment. Nudges that are meant for activating a desired target behavior to which an individual is normally indifferent or inattentive (e.g., nudges to promote organ donation or to discourage from littering). Information security awareness poster with nudges can be considered under this classification.
2. **Externally imposed vs. self-imposed**—Nudges under this dimension determine how an individual adopts a nudge, which could be in two ways—voluntarily (self-imposed) or under the influence of an external option without any compulsion.
3. **Mindful vs. mindless**—Nudges under this dimension try to influence the behavioral outcome of an individual by reaching their inner selves. Mindful nudges are designed to cause a behavioral change consciously in an individual. On the other hand, mindless nudges try to bring about behavioral changes unconsciously. A mindful nudge could be a behavioral change that a person might have been consciously wanting for a while such as eating healthy or quitting smoking. An interesting application of a mindless nudge can be seen when a website tries to set a default choice while signing into a service.

4. Encourage vs. discourage—These nudges strive to bring a behavioral change that is encouraging a specific desired behavior or discouraging a behavior that is believed to be undesirable.

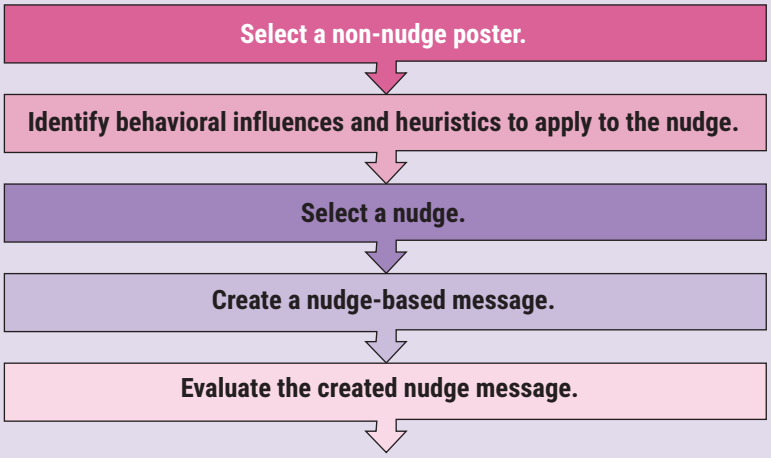
Nudges can be employed by various stakeholders such as the government, organizations and individuals and can result in a range of outcomes. Nudges aim to improve behavior through a broad variety of techniques such as financial incentive, providing relevant information or even actively blocking an inappropriate choice. A few examples of the application of nudges in many real-life scenarios include the following:

- Reduce energy consumption—Consumption of electricity in the US State of California was reduced by nearly 3 percent when residents were nudged by being informed of their electricity consumption in relation to the consumption of other households in that neighborhood.[10]
- Increase expected voter participation in elections—In the US States of New Jersey (2005 general election) and California (2006 primary election), a study was conducted in which voters were nudged using a phone campaign with a mindless encouragement nudge that higher voter turnout is expected. The results showed seven percent of respondents informed the researchers that they were 100 percent likely to vote due to the higher voter turnout nudge.[11]
- Improve tax collection—In 2012, the UK HM Revenue and Customs department tried nudging their delinquent taxpayers by sending reminders in the mail that included a social proof heuristic such as "Nine out of 10 people in the UK pay their taxes on time. You are currently in the very small minority of people who have not paid us yet." Results of such nudge messages were very encouraging, and the UK tax department received payments of £4.9 million from almost 120,000 delinquent taxpayers.[12]
- Reduce speeding tendencies among teenage drivers—In 2013, the US State of Pennsylvania Department of Transportation tried to use the anchoring and adjustment bias heuristic by including images and statistics of road accidents caused by teenage drivers speeding from 2007 to 2009 in the Pennsylvania driver's manual. The salience and vivid nature of the pictures were expected to induce the behavioral change of reducing the teenagers' overconfidence in their driving skills.[13]

Applying Nudge Theory in Information Security Awareness

A possible application of nudge theory in information security management is in improving information security awareness training among the different stakeholders of an organization. An important element of an information security awareness program is the creation of posters that convey messages denoting the information security risk involved while engaging in daily business operations. Security posters can be designed using aspects of nudge theory, particularly encouraging and discouraging nudges. A flowchart (**figure 1**) for

Figure 1—Flowchart for Nudge Poster Conversion



Enjoying this article?

- Read *COBIT Focus Area: Information Security*. *www.isaca.org/COBIT-Focus-Area-Information-Security*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

converting a non-nudge-based poster into a nudge-based poster has been developed after studying nudge creation techniques discussed in published sources.[14, 15]

Select a Non-Nudge-Based Message
The first step in nudge-based poster creation is to identify the message that needs to be conveyed to the employee or customer that is related to information security awareness training. The emphasis should be to check whether the selected message can be presented with a choice architecture that might result in an intended behavioral change.

> "WHEN SELECTING A NUDGE FOR DESIGNING AN INFORMATION SECURITY AWARENESS POSTER, CONSIDER USING ENCOURAGING OR DISCOURAGING NUDGES."

Identify Behavioral Influences and Heuristics to Apply the Nudge
The main task in this step is to identify the bottlenecks that prevent an individual from choosing the desired behavioral choice. In the context of information security awareness training, it could be a lack of seriousness from the part of the employee regarding a particular security risk, or it could be a shortage of information regarding the damage that can be caused due to the occurrence of a security breach. Once the bottlenecks are identified, then nudges can be chosen. When designing a nudge poster, the possible behavioral influences that can be evaluated are loss aversion, confirmation bias and information overload. The following heuristics may be applied while developing a nudge: representativeness, anchoring and adjustment, and social proof. The representativeness heuristic denotes the use of similar attributes to judge the likelihood of an event occurring. Anchoring and adjustment heuristics use an approach of fixing an anchor or reference to make an estimate by applying suitable adjustments. In social proof heuristics, an individual looks at the behavior of their peers and tries to adapt their behavioral pattern to conform to the social norms.

Select a Nudge
Selecting the right nudge is very important. When selecting a nudge for designing an information security awareness poster, consider using encouraging or discouraging nudges. A nudge message can be created with anchoring and social proof heuristics, which can be encouraging or discouraging in nature.

Create the Nudge-Based Poster
Once the nudge dimension has been finalized and the nudge message is selected, the next step is to create the poster. The nudge poster may be slightly different from a conventional poster design because it is expected to elicit a certain behavior from the employee.

Evaluate Effectiveness of the Nudge-Based Poster
After rolling out a nudge-based information security awareness poster, it is important to evaluate its effectiveness by conducting an outcome evaluation exercise using metrics related to the behavior goal of the nudge. It should be noted that just the creation of a nudge-based poster might not result in improving overall information security compliance. Nudge-based posters may fail to achieve the desired objectives due to several reasons. The primary reason for a nudge failure can be linked to the error in identifying the behavior influences of the target employee. Another reason for nudge failure may be the error in applying the relevant heuristics while developing a nudge. If it is found that the nudge-based poster has not achieved its desired effect, the designers of the poster should go back to the drawing board and start tweaking the poster by repeating the steps in the nudge creation process flowchart. Feedback should also be collected from employees about the nudge message, checking if employees could connect themselves with the nudge heuristics applied in the design phase.

Example of Developing a Security Awareness Poster With Nudges

To initiate the conversion process using the flowchart in **figure 1**, a non-nudge poster that was intended to create awareness about password safety was selected. The behavior influence that may be considered is loss aversion, which is the tendency of people to be more attuned toward losses than gains. While developing the nudge, the

heuristic of anchoring and adjustment may be used, which highlights a particular value to influence a behavioral change. Accordingly, two nudges, one with an encouraging nudge dimension and one with a discouraging nudge dimension, were developed. The message in the first poster (**figure 2**[16]) was designed to dissuade employees from using weak passwords using an anchoring heuristic message from a data breach investigation report regarding loss created by weak and insecure passwords. The message in the second poster (**figure 3**) was created using an encouraging nudge dimension with a social proof heuristic in which peer behavior is used to influence behavioral change.

Conclusion

The importance of information security awareness has increased only in current times. Every organization should come up with new and innovative mechanisms to ensure that their different stakeholders are provided with the best possible security awareness training. Organizations should aim to achieve a Security Awareness Maturity Model of level three or above as defined by the SANS Institute, and security awareness programs that encourage behavioral changes should be planned and delivered by organizations.[17] Nudge theory, which has been tried and tested in many different governments, enterprises and other domains, may be considered for improving security awareness training. Bringing about behavioral changes using nudges to alter choice architecture through subtle messages rather than by enforcing action is an option for many organizations. The proposed flowchart for the development of a nudge-based security poster is an effort to introduce new ideas in developing information security awareness training materials. The introduction of new methods for developing awareness posters can improve the effectiveness of security awareness training programs, which in turn helps organizations attain a higher level of information security preparedness.

"BRINGING ABOUT BEHAVIORAL CHANGES USING NUDGES TO ALTER CHOICE ARCHITECTURE THROUGH SUBTLE MESSAGES RATHER THAN BY ENFORCING ACTION IS AN OPTION FOR MANY ORGANIZATIONS."

Acknowledgment

The infrastructural support provided by FORE School of Management (New Delhi, India) is gratefully appreciated.

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*

Figure 2—Example of Nudge-Based Poster 1

Image source: "Secure Data - Cyber Security -" by perspec_photo88 is licensed under CC BY-SA 2.0

Figure 3—Example of Nudge-Based Poster 2

Image source: "Cyber Security - Tablet" by perspec_photo88 is licensed under CC BY-SA 2.0

2 Quagliata, K.; "Impact of Security Awareness Training Components on Perceived Security Effectiveness," *ISACA Journal*, vol. 4, 2011, *https://www.isaca.org/archives*
3 European Union Agency for Network and Information Security, *Cyber Security Culture in Organisations*, Greece, 2017, *https://enisa.europa.eu/publications/cyber-security-culture-in-organisations*
4 *Ibid*.
5 Thaler, R.; C. Sunstein; *Nudge: Improving Decisions About Health, Wealth and Happiness*, Penguin Group, USA, 2009
6 Kosters, M.; J. Van der Heijden; "From Mechanism to Virtue: Evaluating Nudge Theory," *Evaluation*, vol. 21, iss. 3, 7 July 2015, p. 276–291, *https://journals.sagepub.com/doi/abs/10.1177/1356389015590218*
7 Sunstein, C.; R. Thaler; "Libertarian Paternalism Is Not an Oxymoron," *The University of Chicago Law Review*, vol. 70, issue. 4, 2003, p. 1159–1202
8 Mancino, L.; J. Guthrie; "When Nudging in the Lunch Line Might Be a Good Thing," United States Department of Agriculture (USDA), 1 March 2009, *https://www.ers.usda.gov/amber-waves/2009/march/when-nudging-in-the-lunch-line-might-be-a-good-thing/*
9 Ly, K.; N. Mazar; M. Zhao; D. Soman; A Practitioner's Guide to Nudging, Rotman School of Management Working Paper No. 2609347, 23 May 2015, *https://doi.org/10.2139/ssrn.2609347*
10 Rasul, I.; D. Hollywood; "Can Nudges Help to Cut Household Energy Consumption?," *The Guardian*, 27 January 2012, *https://www.theguardian.com/sustainable-business/behaviour-change-energy-consumption*
11 Gerber, A. S.; T. Rogers; "Descriptive Social Norms and Motivation to Vote: Everybody's Voting and So Should You," *The Journal of Politics*, 2009, *https://ssrn.com/abstract=1837781*
12 Calvo-Gonzalez, O.; A. Cruz; M. Hernandez; "The Ongoing Impact of 'Nudging' People to Pay Their Taxes," World Bank Blogs, 2 December 2018, *https://blogs.worldbank.org/voices/ongoing-impact-nudging-people-pay-their-taxes*
13 Acquisti, A.; I. Adjerid; R. Balebako; L. Brandimarte; L. F. Cranor; S. Komanduri; P. G. Leon; N. Sadeh; F. Schaub; M. Sleeper; Y. Wang; S. Wilson; "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online," *ACM Computing Surveys,* vol. 50, iss. 3, 2017, p. 1–41
14 Marcus, A.; E. Rosenzweig (Eds.); *Design, User Experience, and Usability, Interaction Design*, Springer, USA, 2020
15 *Op cit* Ly *et al*.
16 Verizon, *2017 Data Breach Investigations Report 10th Edition*, USA, 2017, *https://enterprise.verizon.com/resources/reports/2017_dbir.pdf*
17 Cassels, W.; K. Alvero; R. Pierson; "A Heightened Sense of Awareness," *ISACA Journal*, vol. 6, 2018, *https://www.isaca.org/archives*