How to Increase Cybersecurity Awareness

The development of information and communication technology is growing at a fast pace. As a result, the Internet has become easy to access. Consequently, the number of Internet users has increased enormously. However, most users are not aware of how important it is to protect their data privacy on the Internet, especially as technology is constantly evolving. Moreover, users have encountered many types of threats that are associated with the Internet, but they may not be aware of them. Therefore, it is crucial to assess the risk associated with user behavior.

It cannot be denied that the Internet is important to everyday life. Almost all work, in both the public and private sectors, relies on IT systems. Hence, systems must be secured and protected. Though there are techniques and policies that can be used to control users’ behaviors, they are not always successful. This is because users are not aware of many risk factors and how to protect themselves from or handle the risk properly. Phishing is a social engineering technique that aims to steal users’ confidential information such as user IDs, passwords, and banking and credit card details. Phishing is a social engineering technique that aims to steal users’ confidential information such as user IDs, passwords, and banking and credit card details. Typically, victims receive an email to lure them to a fake or malicious website that asks for their identifying information. The attack forms are changing every day, and phishing is considered one of today’s most serious threats.

Most public records data that governments have such as name, date of birth, tax identification number, passport number and healthcare details are sensitive. Sensitive data related to national security include military intelligence, civil defense, emergency plans and critical infrastructure protection. Many cyberattacks target third parties to gain access to national security data. Every country is at risk of strategic cyberattacks, which is very challenging. Neither the public nor private sectors can avoid the threat of cyberattacks, which means they must find ways to handle threats properly and effectively.

The US National Institute of Standards and Technology (NIST) provides a description of security awareness in NIST Special Publication (SP) 800-16, which explains that raising awareness is not just about providing a training program; its main purpose is to raise the awareness of people to understand and respond to cyberthreats appropriately.

Nipon Nachin, CISA, CISM, CISSP, CSSLP, GICSP, GREM, ITIL v3 Expert, QSA, PCIP, SSCP
Is a security professional with 16 years of experience. He has worked at ACIS Professional Center as the chief executive officer. He is currently enrolled in the Technopreneurship and Innovation Management Program in the graduate school of Chulalongkorn University, (Bangkok, Thailand) where he is studying for a Ph.D. He can be reached at nipon@acisonline.net.

Chatpong Tangmanee, Ph.D.
Is professor of statistics and information systems on the faculty of commerce and accountancy at Chulalongkorn University. He can be reached at chatpong@cbs.chula.ac.th.

Kerkr Piromsopa, Ph.D.
Is professor of information security in the department of computer engineering at Chulalongkorn University (Bangkok, Thailand). He can be reached at Krerk.p@chula.ac.th.
Government agencies and the private sector have dedicated significant resources to ensure information security. However, technology alone is not sufficient to solve the problem as people are the critical target of the cyberattack, and most of the time, this is not taken into consideration. Therefore, in general, it is imperative to establish an information security policy to protect the security of information and assets by providing an operational framework in addition to laws, regulations and best practices for proper use of information technology. Even when there are training programs in place, there are still cyberincidents; that is, training programs may not be effective enough to solve the problem of cyberattacks.

The main objective of any policy or programs designed to protect information should be to gradually change people’s behaviors. The security protection strategy should be able to identify the critical behaviors that potentially drive behavioral change. In general, for a training program to increase security awareness, people should be required to take pretests and post tests to measure their level of knowledge of cybersecurity threats and demonstrate that they know how to protect themselves from cyberattacks. Though they may know the answers when tested, they may not act accordingly in real life. In addition to training, there are other resources such as videos, websites and security publications that can be used to increase security awareness. However, there is not much research to evaluate which method is the most effective for raising cybersecurity awareness. Therefore, the objectives of this research are to determine the most effective training methods and to develop a prototype that can effectively increase cybersecurity awareness.

Research Related to Raising Cybersecurity Awareness

There are various methods used to increase awareness of cybersecurity, including security awareness posters displayed at an organization, security awareness content on an intranet website, information on a screensaver, in-class training, videos, simulations and tests. According to one study, raising awareness using the intranet is the most effective among the methods listed. Raising security awareness requires that users understand the organization's security policy. In addition, a new method to build security awareness by sending a fake malware email to test the user's awareness has gained attention from the public recently. Using games to build awareness is another effective method; however, it is not as effective as using videos.

According to some research, the factors affecting security awareness are subjective norm attitude, threat appraisal and coping appraisal. Subjective norm attitude is what a person perceives the expectations from others are and how that will have an influence on what behavior he or she will perform. Threat appraisal describes an individual's assessment of the level of danger posed by a threatening event, and coping appraisal is a person's assessment of his or her ability to cope with and avoid the potential loss or damage arising from the threat.

Furthermore, intrinsic benefits, safety of resources, rewards, work impediments, intrinsic cost, vulnerability of resources and sanctions have an impact on operational behavior and compliance with the security policy.

The study discussed herein is divided into three parts. The first part aims to determine the effective methods of raising awareness among five methods, which are classroom training, video clips, intranet, games and a simulation based on survey data. In the second part, the top two most effective methods obtained in the first part of the study are used to test selected organizations in Thailand to determine which method provides the highest level of security awareness. Finally, the last part is focused on developing an effective training program.
that raises security awareness using the results from the previous two parts.

The survey data were collected from people during the 17th Annual Conference of Information Security and Cybersecurity in Thailand. The one-way analysis of variance (ANOVA) is used to find the difference in means of scores of security awareness. The scores of security awareness are the response variables.

The factor considered in this study is the methods used to raise security awareness. There are five methods examined:

- Conventional delivery method
- Instructor-led delivery method
- Online delivery method
- Game-based delivery method
- Simulation-based delivery method

There are six types of security awareness (each has its own score) considered in this research. The one-way ANOVA was performed on the same factor but different responses (or different types of security awareness). The six types of security awareness studied in this research are:

- Knowing the vulnerability
- Realizing an impact when being attacked
- Recognizing that one can be attacked at any time
- Ability to protect oneself during a real incident
- Cyberresilience
- Recognizing the importance of cybersecurity

According to Figure 1, the simulation-based delivery method is the most effective compared to the other four methods because it has the highest scores for all types of security awareness. Also, it can be seen that some factors that have an effect on cybersecurity awareness have more than one check mark; this indicates that the means of scores for those methods are not statistically different.

Based on these results, the top two most effective methods are simulation-based delivery and instructor-led delivery methods, respectively.

In the second part of the study, the two methods obtained in the first part were used to test organizations in Thailand to find the most effective method of raising security awareness. The population of the study is the national critical infrastructure organizations as listed on the announcement of Electronic Transactions Act B.E.
The sample of 20 organizations was randomly selected using a systematic sampling. The awareness presentation used in the training provided readers with knowledge of cyberthreats and phishing attacks. Phishing was simulated in the cloud system, and a fake email was sent to the users in those organizations.

The users of each selected organization were divided into two groups of 100 people. Each group received one type of training. Both groups received a phishing email before the training. The instructor-led delivery method was used on the first group. At the three-hour training, the material covered the topics of cyberthreats, risk behaviors related to the threats, impact of the threats and preventive measures. The simulation-based delivery method was used with the second group. This group was also attacked by phishing before training; however, the results of the attack were discussed during the training, along with how the people in this group could protect themselves from the threats. After the training for both methods, another attack was sent to compare the levels of cybersecurity awareness before and after training. If a user opens, clicks or fills out the information on the phishing email, he or she will get a risk score of 2, 3 or 4, respectively. If the user does nothing, he or she will get the risk score of 1. The risk and awareness have an inverse relationship. Therefore, the lower the risk score, the higher the level of cybersecurity awareness.

In this study, a total of 4,523 employees from 20 organizations, including regulatory agencies, banks, Internet and network providers, airlines, and public services, comprised the sample. A paired t-test was used to compare the means of differences of risk score before and after training.

The independent t-test was then used to compare the results of the two methods. All the tests were done at a significance level of 0.05, meaning that the test concludes that there is a difference between the means of the risking scores, but in fact they are not different. Based on the results, it can be concluded that the simulation-based delivery method can increase the level of awareness and is more effective than an instructor-led delivery method in terms of raising awareness. However, to build security awareness effectively, both methods should be integrated and applied to organizations as they could increase the chance of successfully building security awareness. Furthermore, a large organization can have more than 1,000 employees, which makes applying the instructor-led delivery method difficult. An integrated method of simulation-based delivery and online delivery training may be used, which could easily cover everyone in the organization and also can help easily determine the overall level of the security awareness of the organization.

The third part of the study focused on the prototype development for assessing and enhancing cybersecurity awareness. First, the prototype concepts are developed based on the technology threat avoidance theory (TTAT), which outlines the factors that have an influence on avoidance of cyberthreats.

These factors are threat appraisal, coping appraisal and coping. In addition to TTAT, the requirement of laws and regulations, cost feasibility, capability of risk mitigation, and compliance with standards are considered in the service innovation concept development as well. Thus, there are four alternatives of the prototype concept developed. For alternative 1, the users are trained and then the simulated attack is sent to them after the training, and the result is sent to their supervisor. For alternative 2, the simulated attack is sent to the users and, if they are a victim, they will be sent to an online training program. After training, they are required to take an exam. The process is continuously repeated, and if any user passes the qualification specified by their organization, they will receive a certificate of cybersecurity awareness. For alternative 3, the simulated attack is sent to the users and the result is reported to their supervisor. Finally, alternative 4 is similar to alternative 2, except for there is no certificate. To select the most acceptable alternative, two evaluations were performed. The first evaluation, which aims to obtain information related to a potential prototype concept, is based on the opinions and judgments of
12 specialists in cybersecurity, IT and marketing. The other evaluation focuses on a consumer’s decision to select the service. Using both results from the evaluations, the most acceptable prototype is obtained.

The integration of threat simulation and training through online learning received the best evaluation. Using this result, the prototype for assessing and enhancing cybersecurity awareness is created. Moreover, the acceptance test is performed on the prototype. Fifty users were randomly selected to provide their attitudes and opinions toward the prototype after using it. The result of the acceptance test is used to improve the prototype, and the final version of the prototype is shown in figure 2.

According to figure 2, the simulated cyberthreat is generated and sent to attack employees without informing them in advance, as that would make them aware of the situation. The next step is when the employees decide whether to open the simulated email, which can be used to measure avoidance motivation and behavior according to TTAT. If employees decide to open the email and fill out the information, there is a warning message to inform them that they are victims of the attack and are required to take an online learning course. The online learning course provides the knowledge on various types of cyberthreats, their impacts and how to protect against cyberthreats and attacks. After finishing the online learning course, employees are required to take an online exam to evaluate their perceived susceptibility, perceived severity, perceived effectiveness, perceived costs and self-efficacy. If the employees pass both the simulation and exam, it means that they have an acceptable level of cybersecurity awareness, which may lead them to find a way to protect themselves against cyberthreats.

**Figure 2—The Prototype for Assessing and Enhancing Cybersecurity Awareness**
Conclusion

Many organizations provide training programs to increase their cybersecurity awareness. However, the training may not be enough for organizations to cope with cyberthreats and attacks. Because most cybersecurity awareness programs focus on theory, they cannot build cybersecurity awareness and an incident response process. That is, besides a training program, it is important for employees and management to experience life-like cyberincidents, which are similar to a fire drill and are called cyberdrills. The cyberdrill is a training process that simulates a cyberattack on employees or people whose work is related to cyberincident response. These drills make them more familiar with the threats. Moreover, cyberdrills can determine if an employee has a high risk of being a victim of cyberthreats. A rapid response for an incident leads the organization to a state of cyberresilience that is very robust against the impacts of attacks. This kind of response can help the organization maintain the service level agreement (SLA) with customers. Therefore, the cyberdrills can help make employees in the organization aware of cyberthreats and provide more efficient responses to them.

Endnotes


