# Designing a Security Awareness and Training Program

Steven Christopher Wong

School of Computer Science, Northcentral University

TIM 8301 v4:  Principles of Cybersecurity

Dr. Lynn Lazar

September 18, 2022,

## Designing a Security Awareness and Training Program

This document will discuss the design of a security awareness and training program. In this report, the staff will describe the level of education and professional development necessary for employees involved in the management of cyber-security implementations in the company. This document outlines each competency for each concentration. An educated and uneducated audience to build awareness and remind everyone that there is still a problem. Using the National Institute of Standards and Technology SP 800-50 document as a reference and best practices for building the program, this document will be used as a resource for weekly resources. This document will describe how the program supports appropriate governance, risk, and strategies to comply with government audits and regulations for improving data protection within the company. Justifications for each best practice and recommendation will be supported by the National Institute of Standards, Technology Cybersecurity Framework, and other industry-accepted standards.

## Education

Repeat instructional messages and make educational materials engaging and current. Using various techniques of communicating this information can dramatically raise user awareness of the lesson or problem. Consider an instructor-led course on how to prevent being a victim. Posters and regular emails may be used to spread his thoughts across the whole

institution as part of social engineering scams. This corporation, as a software and hardware vendor, and other institutions should collaborate on these university certification programs. The corporation must work with educational institutions to deploy personnel to schools and train instructors in order to minimize cybersecurity risks across the company (*Building an information technology awareness and training program, 2003)*.

## Training

The National Institute of Standards and Technology Special Publication 800 defines training as the level of a learning continuum in which practitioners in operational specializations other than information technology attempt to build and need security skills and know-how (*Building an information technology awareness and training program, 2003)*. Training skills lay the groundwork for educational awareness, notably in the areas of security and literal documents. A training program does not always result in a degree or certificate from a higher education institution.A training course, on the other hand, might contain the same knowledge as a collegiate course with a certificate or program for a degree. An IT security course for system administrators is an example of training. This course requires me to explain the administrative, operational, and technical controls that must be implemented. Administrative rules include policy, IT security program management, risk management, and life cycle safety; operations management includes issues with staff and users, contingency planning, incident handling, awareness and training, computer support and operation, and physical and environmental

security. Identification and authentication, logical access restrictions, and audit trail encryption are examples of technical controls.

The development of training materials that offer the skill set(s) required for participants to carry out the security duties related to their occupations is recommended. For someone studying a new field (like system administration), IT security training materials can be created at an introductory level. administrators of email or web servers, auditors). The development of material at the intermediate level for someone who has greater responsibility and expertise in a subject. Advanced For those "centers of excellence" or agency subject matter specialists whose positions require them to generate content with the highest degree of trust and the corresponding degree of responsibility for IT security.

**Awareness**

Activities aimed at changing behavior or enforcing security best practices are examples of safety awareness activities. Consciousness is defined as "Awareness is not training," according to National Institute of Standards and Technology Special Publication 800-16. The Goal of Consciousness The purpose of the presentation is to draw attention to the importance of safety. Individuals are empowered by awareness presentations to detect and respond to IT security risks. Training does not replace awareness. The goal of awareness presentations is to draw attention to safety concerns. Allow for presentation of IT Security Certification Please examine and answer

the questions according to Special Publication 800-50 of the National Institute of Standards and Technology.

The learner is the recipient of information in awareness exercises, whereas the learner is the learner in training. The surroundings become more lively. Reaching a large audience with compelling content packaging technology is what awareness is all about. Training is more formal and focuses on developing knowledge and skills to make jobs simpler. Virus prevention is an example of a topic for an awareness session (or awareness material supplied). This subject may be tackled succinctly by outlining what viruses are and what they are capable of.What happens if a virus attacks your computer? What should be done if a virus is discovered? Special publications from the National Institute of Standards and Technology serve as a bridge or transitional period between awareness and training. Safety concepts and knowledge are addressed in 800-16. Terms, subjects, and concepts are all part of the primary literacy material. Once an organization has established a program to improve its overall level of security, awareness, and vigilance, foundation and literacy materials allow for the formation or development of more robust awareness.

**Model 3 Awareness Training Program**

Policy and budget are handed over from Organizational units receive policy and budget approval from the head office.units carry out their own development training plan. The organizational unit develops awareness and training materials and A method for using materials

in their own units.Unless the central authorities have something very good Strategies for policy and program requirements Implementation and performance may be considered and unit-level operational issues Fully decentralized program management model Possibly "throwing the IT security program overboard Walls with little to no accountability". Similar to the centralized program management model (Model 1) and the partially decentralized program management model, Program Management Model (Model 2), Central Authority and In this model, organizational units move in both directions.

The central government Government agency policies on IT security awareness and training, as well as their specific budgets. The central authority should request that the organizational units be in charge of undertaking unique requirements analysis, strategy formulation, and training development. Program development and implementation Alternatively, central authorities can give advice, and organizational unit training can perform their tasks.Central agencies may seek contributions on a regular basis. Budget expenditures made by each organizational unit, status and outcomes Analysis of needs given a chosen plan Reports on organizational unit progress, training plan status, and training delivery Materials for raising awareness and training.Reports from organizational units can also be requested by central authorities.

NIST Special Publication 800-50 number of individuals who have participated in awareness sessions, number of people who have been trained on certain themes, number of people who have not yet attended an awareness and training event This completely decentralized

program management technique is widely employed by organizations such as: Large in comparison. It features a highly dispersed organization, with the headquarters allocated general duties (central). At the unit level, certain tasks are allocated. The functions are dispersed across a vast geographical region. Also, they have semi-autonomous organizational units with distinct and distinct tasks. Furthermore, training programs may require major changes. The technique is to undertake a requirements analysis after the model to be used has been determined. Defined in accordance with the organizational model chosen.

## Justifications for Each Recommendation

The following section will justify why these awareness and training methods can be useful to this company. Newsletters, videotapes, web-based sessions, computer-based sessions, teleconferencing sessions, in-person instructor-led sessions, and brown bag seminars are all messaging tactics.Low-cost solutions include messaging on awareness tools, posters, access lists, "do and don't lists," checklists, screensavers and warning banners, desk-to-desk cautions, agency-wide e-mail messages, in-person instructor-led sessions, brown bag seminars, and reward programs. Using multiple communication approaches to convey this information can significantly increase user awareness of the lesson or problem. Social engineering attacks may be advanced by employing posters and regular emails to propagate his ideas across the institution. Consider taking an instructor-led seminar on how to avoid being a victim.

## References

ComplyUP, C. U. (2022, March 25). *Compliance overview: CMMC & NIST 800-171*. ComplyUp. Retrieved September 18, 2022, from https://complyup.com/compliance-overview/?utm_campaign=CU20%2B-%2BStatic%2BCMMC%2BSearch%2BCampaign&utm_source=bing&utm_medium=ppc&utm_term=cyber+security+nist+800+171&hsa_acc=8381633541&hsa_cam=11146093633&hsa_ver=3&hsa_net=adwords&hsa_src=o&hsa_tgt=kwd-79371490763765%3Aloc-190&hsa_grp=1269936706442249&hsa_ad=&hsa_kw=cyber+security+nist+800+171&hsa_mt=b&msclkid=c78e24f529c71dd06d4747d2e2ceeedf

National Institute of Standards and Technology. (2003, October). *Building an information technology awareness and training program.* NIST.

Warsinske, J., Graff, M., Henry, K., Hoover, C., Malisow, B., Murphy, S., Oakes, C.P., Pajari, G., Parker, J.T., Seidl, D., & Vasquez, M. (2019). *The official (ISC) 2 guide to the CISSP CBK Reference* (5th ed.). Wiley.