


Chapter 29

Delivering Effective Cybersecurity Awareness Training to Support the Organizational Information Security Function

Regner Sabillon

 <https://orcid.org/0000-0003-1807-2208>

Universitat Oberta de Catalunya, Spain

ABSTRACT

Traditional security education, training, and awareness (SETA); cybersecurity awareness programs; and information security awareness programs are falling behind to deal with the current cyberthreat landscape in any organizational environment. Human behaviors are the weakest links in cybersecurity, especially in situations where cyberthreats are not isolated, blocked, or reported to the information security specialists for further action. Moreover, the study compares recent awareness frameworks, approaches, and methodologies. An extended research that includes an awareness training model to deal with existing challenges when delivering cybersecurity to different levels of positions in any organization. The cybersecurity awareness training model (CATRAM) has been designed to deliver training to different organizational audiences, each of these groups with specific content and separate objectives. The study concluded by addressing the need for future and innovative research to target new approaches to keep cybersecurity awareness focused on the everchanging cyberthreat landscape.

INTRODUCTION

A comprehensive Information Security Program must include Security Education, Training and Awareness (SETA). One of the main responsibilities of the Chief Information Security Officer (CISO) is to design and implement a successful and measurable SETA in any corporate environment. SETA aims to reduce

DOI: 10.4018/978-1-7998-8954-0.ch029

the occurrence of accidental cybersecurity breaches by members of any organization including Board of Directors, C-Suite Executives, Managers, Employees, Consultants, Vendors and Business Partners who are working with its cyber assets.

Cybersecurity awareness training programs may not be productive if people's behavior remain unchanged, and as result a positive corporate impact cannot be achieved. A cybersecurity awareness program is an organizational long-term investment, that will help to establish a cybersecurity culture if training is delivered on a continuous basis with relevant content that is aligned with the current cyber threat landscape. Cybersecurity directors could envision a more interactive experience that will allow staff to be more proactive beyond the point of dealing with cyber incidents and cyberthreats.

We consider that the Cybersecurity Awareness TRaining Model (CATRAM) can represent a substantial foundation for the implementation of any organizational cybersecurity awareness program. CATRAM can also assess any awareness training model that is persistent and relevant with the current cyberthreat landscape.

Whitman and Mattord (2019) highlight that a SETA program consists of security education, security training and security awareness. Organizations may or may not able to develop an in-house SETA program and would consider to outsource to educational institutions or Companies specializing in delivering security training. SETA programs are implemented to build in-depth knowledge for organizational security programs and protection of information assets, to develop skills for end users so they can perform their job responsibilities with security in mind and by improving security awareness for the protection of information assets.

According to Whitman et al. (2019), a SETA is defined as:

A managerial program designed to improve the security of information assets by providing targeted knowledge, skills, and guidance for organizational employees.

Security Awareness, Security Education and Security Training are the main components of any SETA program. *Security Education* consists of delivering the knowledge of information security issues and operations, *Security Training* provides participants with skills, knowledge and abilities to user their assigned resources in a wise manner and *Security Awareness* refers to create consciousness when dealing with InfoSec or cybersecurity matters.

Regardless of any cybersecurity control or security measure, users are recognized as the existing weakest link in securing systems and in the aftermath, they are not aware that the consequences of their actions may affect information security (NIST SP 800-12, 2017). Pendergast (2016) also suggests that employees are responsible for the financial losses caused by cybersecurity incidents and data breaches.

According to the NTT Group (2017), integrating cybersecurity processes can empower digital transformations of any organization based on the maturity level of their digital transformation projects. By doing so, Companies will identify and control cyber risks, reduce complexity of cybersecurity architecture for their business operations, add value to their digital business, define the prioritization of areas to deal with business-critical cyber risks and plan a cyber resilience plan for the digital transformation.

A recent study from Fujitsu (2017), that evaluated the digital transformations from 1,625 decision makers in different industries and sector across fourteen countries concluded that 86% of the participating organizations have a clear digital strategy that includes abilities to address cybersecurity issues. Moreover, 52% of these organizations are investing in cybersecurity or 51% in implementing Internet of Things (IoT) to strengthen their digital transformations.

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/delivering-effective-cybersecurity-awareness-training-to-support-the-organizational-information-security-function/280197

Related Content

Applied Cryptography for Security and Privacy in Wireless Sensor Networks

Dulal C. Kar, Hung L. Ngo and Geetha Sanapala (2009). *International Journal of Information Security and Privacy* (pp. 14-36).

www.irma-international.org/article/applied-cryptography-security-privacy-wireless/37581

A Distributed and Secure Architecture for Signature and Decryption Delegation through Remote Smart Cards

Giuseppe Cattaneo, Pompeo Faruolo and Ivan Visconti (2012). *Threats, Countermeasures, and Advances in Applied Information Security* (pp. 53-65).

www.irma-international.org/chapter/distributed-secure-architecture-signature-decryption/65762

Privacy through Security: Policy and Practice in a Small-Medium Enterprise

Ian Allison and Craig Strangwick (2008). *Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions* (pp. 157-179).

www.irma-international.org/chapter/privacy-through-security/6865

Data Leakage in Business and FinTech

Usama Habib Chaudhry, Razi Arshad, Naveed Naeem Abbas and Adeel Ahmed Zeerak (2023). *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications* (pp. 192-207).

www.irma-international.org/chapter/data-leakage-in-business-and-fintech/314081

DoS Attacks on RFID Systems: Privacy vs. Performance

Dang Nguyen Duc and Kwangjo Kim (2013). *Advanced Security and Privacy for RFID Technologies* (pp. 139-152).

www.irma-international.org/chapter/dos-attacks-rfid-systems/75516