

Chapter 6

Fortifying Corporate Human Wall:

A Literature Review of Security Awareness and Training

Anandharaman Pattabiraman
University at Buffalo, USA

Kaushik Swaminathan
University at Buffalo, USA

Sridhar Srinivasan
University at Buffalo, USA

Manish Gupta
University at Buffalo, USA

ABSTRACT

It has been very evident from data breaches from last few years that attackers are increasingly targeting the path of least resistance to compromise the security of organizations. Cyber security threats that exploit human behavior are becoming sophisticated and difficult to prevent against. At the same time humans are the countermeasures that can adapt swiftly to changing risk landscape than technological and procedural countermeasures. Organizations are implementing and enhancing their security awareness and training programs in an attempt to ensure that risks from human elements, which pose the greatest risks, are mitigated. The chapter conducts a thorough literature review in the area of security awareness and training and presents a classification scheme and a conceptual research model to provide insights into the existing body of knowledge in the area. Trends and analyses are also presented from the reviewed papers, which can be of importance to organizations in improving their security awareness programs. The insights from the study can be leveraged to build a strong human wall against both internal and external threats that are fast evolving and causing tremendous amount of loss.

DOI: 10.4018/978-1-5225-2604-9.ch006

1. INTRODUCTION

Information is the fundamental asset of an organization and hence it is vital to protect the information. Though we have spent heavily on tools such as antivirus software, firewalls, intrusion detection and prevention systems to protect the information security, the threats aren't completely eradicated due to the gaps in the implementation of security tools and due to the reason that not all threats to security are known to the user community. We try to address the same through efficient security training which creates another level of defence for an organization in overcoming the security threats. Most of the times, employees follow organizational policies to ensure compliance however certain gaps are found which compromises the information. Few examples include ignoring the antivirus alerts, leaking out sensitive information through phone, writing passwords in desk, downloading a malicious file, etc. As the deliberate threats to information are prevalent, we deal with necessity of enforcing a strong security program which will help users in understanding the security policies of an organization and to empower the users to protect themselves and the organization from any security issues.

This paper documents the essential business case for investing in a cost-effective security awareness training program. Through proper trainings to user group, we seek to establish a proper culture which complies with the information security policies and goes a long way in helping reduce risks and cut costs for an organization. The training methods could include publishing awareness through emails, newsfeeds, blogs and also through refresher courses and by conducting regular auditing. To analyse the existing security awareness programs in the market, we performed intensive research of several related papers, the details of which have been specified below. These papers help to provide details of the current security training programs in place, the identified security gaps and how theories are framed to ensure that the information security needs of an organization are met.

The contributions of the chapter are many-fold. First it provides a comprehensive view of literature in the area of security awareness and training from last few years. Second, the filtering and classification process provides insight into the trends and emphasis of recent research which has been in response to growing needs for a robust and effective information security awareness program. Given the increasing trend of human link being the weakest and most exploited links, organizations are increasingly adapting their programs to the shifting risk landscape. The chapter shows the pattern of research to indicate the areas in security awareness that have gained importance in recent years. The chapter is organized in 5 sections. Second section provides an overview of security awareness and training, third section provides

32 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/fortifying-corporate-human-wall/183238

Related Content

Socio-Technical Attack Approximation Based on Structural Virality of Information in Social Networks

Preetish Ranjanand Abhishek Vaish (2021). *International Journal of Information Security and Privacy* (pp. 153-172).

www.irma-international.org/article/socio-technical-attack-approximation-based-on-structural-virality-of-information-in-social-networks/273596

AER-Aware Data Aggregation in Wireless Sensor Network Using Hybrid Multi-Verse-Optimized Connected Dominant Set

Santhoshkumar K.and Suganthi P. (2022). *International Journal of Information Security and Privacy* (pp. 1-17).

www.irma-international.org/article/aer-aware-data-aggregation-in-wireless-sensor-network-using-hybrid-multi-verse-optimized-connected-dominant-set/308313

Assessing HIPAA Compliance of Open Source Electronic Health Record Applications

Hossain Shahriar, Hisham M. Haddadand Maryam Farhadi (2021). *International Journal of Information Security and Privacy* (pp. 181-195).

www.irma-international.org/article/assessing-hipaa-compliance-of-open-source-electronic-health-record-applications/276390

Cryptography for the Forensics Investigator

Thomas Martin (2013). *Theory and Practice of Cryptography Solutions for Secure Information Systems* (pp. 62-83).

www.irma-international.org/chapter/cryptography-forensics-investigator/76511

Blockchain and PUF-Based Secure Transaction Procedure for Bitcoin

Sivasankari Narasimhan (2021). *Revolutionary Applications of Blockchain-Enabled Privacy and Access Control* (pp. 172-188).

www.irma-international.org/chapter/blockchain-and-puf-based-secure-transaction-procedure-for-bitcoin/274703