Implication of Employees in Security Policies Definition

Myriam Djerouni
Luxith G.I.E., Luxembourg
myriam.djerouni@luxith.lu

Abstract

A way of awareness is to involve employees in part of the definition of security policies. The purpose of this approach is not to reduce the level of security required and defined by the policies but to consider when it is possible and applicable their comments. In this case, employees accept more easily the application of policies as they have "participated". Then, the policies should be present to employees during interactive sessions with real cases of security breach, figures, and statistics to illustrate the risks. The benefits of these presentations are to show to employees that risks are not only theoretical and it can really happen. The purpose of this document is to provide guidance on how to create more cybersecurity awareness, topic handled by the CyberEDU in February 2019. This paper presents the implication of employees across the life cycle of the security policies based on the PDCA (Plan-Do-Check-Act) model. The document will addresses the definition of Information Security Policy (ISP) as well as topic-specific policies and the involvement of the Top Management and employees.

Index terms: Policy maker, Implication of employees, Security Awareness, Interactive Awareness

References:

[1]. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary, https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

[2]. IOS/IEC 27002:2013[2], Information technology — Security techniques — Code of practice for information security controls

[3]. NIST (National Institute of Standards and Technology)- Glossary of Key Information Security Terms published in 2013, https://www.nist.gov/publications/glossary-key-information-security-terms-1

[4]. Verizon Data Breach Investigation Report, https://enterprise.verizon.com/resources/reports/dbir/