Journal of Cases on Information Technology
Volume 21 • Issue 3 • July-September 2019

An Effective Cybersecurity Training Model to Support an Organizational Awareness Program:

The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada

Regner Sabillon, Universitat Oberta de Catalunya, Barcelona, Spain
Jordi Serra-Ruiz, Universitat Oberta de Catalunya, Barcelona, Spain
Victor Cavaller, Universitat Oberta de Catalunya, Barcelona, Spain
Jeimy J. Cano M., Universidad del Rosario, Bogota, Colombia

ABSTRACT

Traditional cybersecurity, security or information security awareness programs have become ineffective to change people's behavior in recognizing, failing to block or reporting cyberthreats within their organizational environment. As a result, human errors and actions continue to demonstrate that we are the weakest links in cybersecurity. This article studies the most recent cybersecurity awareness programs and its attributes. Furthermore, the authors compiled recent awareness methodologies, frameworks and approaches. The authors introduce a suggested awareness training model to address existing deficiencies in awareness training. 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 authors concluded their study by addressing the need of future research to target new approaches to keep cybersecurity awareness focused on the everchanging cyberthreat landscape.

KEYWORDS

Awareness Training Delivery, Awareness Training Evaluation, Awareness Training, Cybersecurity Awareness Model, Cybersecurity Awareness Program, Cybersecurity Awareness Training, Cybersecurity

INTRODUCTION

A good Cybersecurity Awareness Program must include adequate training that is aligned with the organization's objectives, the focus to raise cybersecurity awareness while performing employee's duties and an interactive communication between all stakeholders for any cybersecurity matter.

Awareness programs may fail if they are not designed to change people's behavior and likewise if a positive impact on any organization cannot be achieved. A cybersecurity awareness program is a corporate long-term investment that will help to create a cybersecurity culture if training is delivered on a continuous basis. A more aggressive vision of the awareness aim is to go beyond the prevention of cybersecurity incidents.

DOI: 10.4018/JCIT.2019070102

We believe that the proposed Cybersecurity Awareness TRAining Model (CATRAM) can represent a solid foundation for the implementation of any organizational cybersecurity awareness program. CATRAM can also review any awareness training model that is consistent and updated with the current cyberthreat landscape.

Despite enough cybersecurity measures, employees continue to be the weakest link in cybersecurity. Staff are directly connected to financial losses related to data breaches and cybersecurity incidents (Pendergast, 2016).

Cano (2016) emphasizes that one of the consequences of current information security training methodologies is the "Bottom-up delegation"; this scenario does not allow end users to practice freedom and autonomy when it comes to data protection but instead follow and abide certain organizational information security policies.

LITERATURE REVIEW

According to the Gartner Magic Quadrant (2016) for Security Awareness Computer-Based Training where leaders, visionaries, challengers and niche players are positioned. The Leaders are SANS Institute, Wombat Security Technologies, PhishMe, MediaPro, Security Innovation, Inspired eLearning, Terranova WW, PhishLine, Global Learning Systems, The Security Awareness Company; Visionary vendors are Popcom Training and Security Mentor; Challenger vendors are BeOne Development, KnowBe4 and Optiv Security and last but not least are niche players like Junglemap, Digital Defense, Symantec (Blackfn Security) and Secure Mentem.

According to the Global Security Awareness Report from SANS (2017), time and communication were identified as the critical takeaways to a thriving awareness program. The findings highlighted poor communication to engage people, the problem of time and lack of resources being assigned to a corporate awareness program. The participants reported that they implemented awareness and behavior change (54.6%), had a compliance awareness program (27.1%), achieved long-term sustainment and culture change (9.8%), defined a program with robust metrics (0.9%) and did not have a cybersecurity awareness program at all (7.6%).

Symantec (2014) argues that poorly trained personnel increases the risks of disclosure and loss of sensitive data like Personal Identifiable Information (PII) and Intellectual Property (IP). Its Security Awareness Program reduces vulnerabilities by creating a corporate culture and train employees to protect any organization critical assets from cyberattacks, exploitation, fraud and unauthorized access. The main topics of Symantec's training program are information security, threats, vulnerabilities, countermeasures, securing the workplace, securing mobile users, protecting Internet information, social media mobile device security.

A research study from Enterprise Management Associates (EMA, 2014) reported that 56% of personnel, not including IT and security staff, have not received any security awareness training in their organizations and 84% of participants recognized that the awareness training from their workplaces was also used to decrease cyber risks at home. Furthermore, the study findings confirmed that the existing security awareness programs lack the appropriate delivery periodicity, content and quality. In addition, Company size, market and budgets have a significant impact on the existence and maturity of their corporate awareness training.

ESET (2017) provides free online cybersecurity awareness training to train employees and get a certification. The topics include an overview of threats like malware, phishing and social engineering; best practices for password management; best practices for email protection and preventive measures that cover best practices for cyber hygiene at the workplace and at home. PhishMe also provides access to a free of charge Computer Based Training (CBT) course called PhishMe CBFree which contains seventeen security awareness modules and four compliance training modules. The course is available in seven languages (English, Chinese, French, German, Portuguese, Spanish and Japanese). The Compliance modules are General Data Protection Regulation (GDPR), Payment Data, Personal Data