

Chapter 21

Techniques and Tools for Trainers and Practitioners

Melanie Oldham

Bob's Business, UK

Abigail McAlpine

Bob's Business, UK

ABSTRACT

If the material is to be delivered effectively, organizations need to understand the human side of cyber security training. In this chapter, the authors draw upon over a decade of experience in creating and adapting training and resources with the help of industry professionals and feedback from clients, which has led to a successful and highly acclaimed approach to cybersecurity education. The resulting discussion considers how to adopt the right approach to cybersecurity training for organizations, with training modules that cater to end users, and which are designed to ensure maximum retention of information by presenting short, humorous, animated scenarios that are relatable for the target audience.

INTRODUCTION

For organizations looking to meet compliance requirements or develop a security conscious workforce, this chapter can be used to provide insight into the different approaches to educating the workforce and the different tools and techniques to help develop an established awareness campaign. Understanding and assessing the needs of an organization is essential for the ongoing engagement of learners' interest in cybersecurity. While awareness campaigns are now becoming more commonplace in organizations many see the information as guidance rather than rules, some may even see it as a tick box exercise and cumbersome to integrate into staffs' roles, also possibly perceived as negatively affecting the performance in their tasks and activities.

DOI: 10.4018/978-1-6684-3554-0.ch021

Techniques and Tools for Trainers and Practitioners

As well as communicating the fundamental teachings of cybersecurity it is also necessary to understand how learners take in information. This chapter presents hints and tips on how to differentiate, plan and manage training sessions, courses and modules to best fit the organization's needs and those of its learners. This tactic allows more informed decisions about how to approach cybersecurity training and the benefits and problems with each tactic. Organizations can utilize combinations of different tactics to teach learners how to be safe and secure when engaging with the digital environment.

It is vital to provide factual and critical information when educating the workforce in the correct attitudes and behaviors to conduct within the organization. Cybersecurity training will also provide skills to navigate themselves more securely online with broader society. Adequate training is more than just providing the facts, and how to apply them, the most effective training changes how learners change their attitudes and behaviors in the long-term, it changes how the individuals engage with others online, their self-awareness and their ongoing interest in the education of cybersecurity. Cybersecurity awareness should not stop once a learner leaves an educational environment. Great training inspires and encourages learners to develop an inquisitive mind, not just for organization security but their personal security and those around them.

All organizations have the opportunity to become cyber secure; this is known as Cybersecurity Culture (CSC) which refers to people's behavior, knowledge, perceptions, attitudes, assumptions, norms and values interacting with technology and devices. Good CSC should encompass an understanding of the current culture within an organization and the gap before the ideal culture. The European Union Agency for Network and Information Security (ENISA) states that CSC should:

Encompasses familiar topics including cybersecurity awareness and information security frameworks but is broader in both scope and application, being a concern with making information security considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions (ENISA, 2018).

This chapter provides practical help and support towards establishing the needs of learners and readers will be asked to consider, reflect and re-evaluate their teachings with feedback from learners. Whether organizations are at the start of the journey of educating their workforce, or part way through, and whether they are handling the training internally or externally, the chapter aims to provide the information required to create an efficient and effective learning plan.

WHY TEACH CYBERSECURITY ONLINE?

Learning is sometimes more useful as an isolated activity; many learners enjoy learning flexibly at their own pace, others prefer to learn in a social context. Using the courses provided by Bob's Business as an example, the aim is to combine the best of both, with online learning being accessible in the office or on the go. Training can be in a group environment, and post-training discussion is encouraged with extra learning re-enforcements and resources.

Although there is now a recognized, established and growing need for cybersecurity training for organizations there is a fundamental lack of understanding of how to treat and educate workforces. An active CSC will drive changes in policy, procedures and everyday activities; the motives for different organizations to conduct cybersecurity training are different across the board. Cyber threat awareness

18 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/techniques-and-tools-for-trainers-and-practitioners/292123

Related Content

Smartphone-Based Virtual Reality as an Immersive Tool for Teaching Marketing Concepts

Haithem Zourrig (2021). *International Journal of Innovative Teaching and Learning in Higher Education* (pp. 1-13).

www.irma-international.org/article/smartphone-based-virtual-reality-as-an-immersive-tool-for-teaching-marketing-concepts/273628

Entrepreneurship Micro-Ecosystems in Practice

Ján Reháč, Rafaela Bueckmann Diegoliand Miguel Angel Rodríguez Montes (2020). *Examining the Role of Entrepreneurial Universities in Regional Development* (pp. 113-132).

www.irma-international.org/chapter/entrepreneurship-micro-ecosystems-in-practice/238506

Empowering Civic Responsibility: Insights From Service Learning

Miftachul Huda, Kamarul Azmi Jasmi, Yabit Alas, Sari Laelatul Qodriah, M. Ihsan Dacholfanyand Ezad Azraai Jamsari (2018). *Engaged Scholarship and Civic Responsibility in Higher Education* (pp. 144-165).

www.irma-international.org/chapter/empowering-civic-responsibility/188575

Incorporating Physics Principles in General Biology to Promote Integrative Learning and Thinking

Tennille D. Presley, Noelle A. Harp, Latrise S. Holt, Destini Samueland Jill JoAnn Harp (2021). *International Journal of Innovative Teaching and Learning in Higher Education* (pp. 1-19).

www.irma-international.org/article/incorporating-physics-principles-in-general-biology-to-promote-integrative-learning-and-thinking/278401

Existing Retention Strategies: Their Shortcomings and Benefits

Samuel L. Hinton (2016). *Setting a New Agenda for Student Engagement and Retention in Historically Black Colleges and Universities* (pp. 1-7).

www.irma-international.org/chapter/existing-retention-strategies/157921