Razvan Beuran

Cybersecurity Education and Training

Springer

Cybersecurity Education and Training

Razvan Beuran

Cybersecurity Education and Training

Springer

Razvan Beuran
Next-Generation Digital Infrastructure
Research Area
Japan Advanced Institute of Science
and Technology
Nomi, Ishikawa, Japan

ISBN 978-981-96-0554-5 ISBN 978-981-96-0555-2 (eBook)
https://doi.org/10.1007/978-981-96-0555-2

To my family and two cats =^.^=

Preface

In the early 2000s, as a fresh Ph.D. student living in France, I returned back to my home country, Romania, for the holidays. Naturally, I took with me the laptop that I had recently purchased and used for a while already. Once I arrived home, I almost immediately connected it to the Internet—via dial-up access, naturally—to read my emails. Almost instantly I noticed some strange network activity, and by some sort of reflex, I disconnected the modem cable. Alas, it was too late, as a virus had already infected my laptop, and every minute or so the computer would keep rebooting itself. What was I to do?!

The only solution I could come up with was to visit one of the early Internet cafés that had popped up in Bucharest and investigate the problem. Luckily, I was able to find some instructions on how to remove that virus by deleting a specific file in the system directory. I then rushed home and used the interval between reboots to follow those instructions as quickly as I could. Imagine my relief when, lo and behold, the virus was gone. Only then I was able to use again my computer normally (after enabling the firewall this time, of course).

Fast forward 20+ years, and I am now doing research on cybersecurity in Japan, one of my topics being cybersecurity education and training. Times have changed, and nobody in their right mind would connect to the Internet on a computer that doesn't have some security software installed. Malware has also evolved, and the chances that you can remove an infection yourself by simply deleting one file are pretty slim. Given the emergence of advanced persistent threats, you'll probably not even notice that your computer is infected. But despite all these changes, my vision of cybersecurity is still driven by that early experience I had when connecting my first laptop to a dial-up network in Romania, as doing practical things by yourself is definitely a *sine qua non* of this field.

Fortunately, I was able to put into play this vision as a member of the Cyber Range Organization and Design (CROND) endowed chair at Japan Advanced Institute of Science and Technology (JAIST) that was established with the support of NEC Corporation from April 2015 until March 2021. The goal of CROND was to advance the field of cybersecurity education and training, especially through conducting research on cyber ranges, the network environments that are typically

used for the hands-on training activities that any cybersecurity professional must undertake.

This book was conceived as a culmination of our research at CROND and I intend it to be a practical instrument that cybersecurity educators and training experts can use to guide their work. To achieve this goal, the book provides a thorough view on cybersecurity education and training, in which theoretical descriptions are interspersed with practical details. Consequently, readers can gain both the theoretical understanding, and the practical information, needed to develop and conduct cybersecurity training activities.

The first part of the book systematizes all the aspects related to cybersecurity education and training methodologies, starting with technical cybersecurity training for professionals, which is discussed in much detail. Moreover, issues related to IoT security training, and the cybersecurity awareness training targeted at regular IT users, are also mentioned. This makes it possible for readers to understand the requirements of developing effective training activities that help participants learn how to deal appropriately with cybersecurity incidents.

The second part of the book focuses on the presentation of actual cybersecurity training platforms, such as Capture The Flag (CTF) platforms and cyber ranges. This is followed by a detailed case study on the integrated cybersecurity training framework CyTrONE that we developed at CROND, and a discussion of training platform capability assessment. Thus, the second part provides all the practical know-how needed to effectively set up cybersecurity training activities.

I hope that readers will find this book useful when addressing the many challenges related to cybersecurity education and training, and I am looking forward to the progress that their own contributions to this field will bring—a progress that is absolutely necessary to fill the significant cybersecurity workforce gap that we are currently faced with.

Nonoichi, Japan Razvan Beuran
August 2024

Acknowledgements

This book would not have been possible without the support of many people. First and foremost, I would like to thank Prof. Yoichi Shinoda and Prof. Yasuo Tan, who gave me the opportunity to come to JAIST as a postdoc in 2005, and later to return as research associate professor in 2015. In this context, I would also like to mention Prof. Ken-ichi Chinen, who has been my main collaborator at the Cyber Range Organization and Design chair at JAIST. Many of the ideas presented in this book were born through the stimulating discussions I had with them.

In addition, I cannot forget all the students in my lab at JAIST who contributed to the many research projects whose accomplishments laid the foundation for this book. They are listed next in chronological order of their study period: Cuong Pham, Dat Thanh Tang, Takuya Inoue, Jidong Wang, Zheyu Tan, Min Zhao, Liangwen Yuan, Zhe Zhang, Youmeizi Zeng, Zhenguo Hu, Tan Duy Le, Sian En Ooi, Quyen Van Nguyen, and Thanh Phuong Huynh Nguyen. Thank you all!

Furthermore, several Chinen lab students, such as Fumikazu Awa, Masanori Sunagawa and Gen Komatsu, as well as minor research project or internship students, such as Muhammad Harith bin Noor Azam, Chunqi Du, Lei Jiang, Kien Chi Vu, Wataru Mishima, Yuichiro Sakamoto, and Yoshiki Makino, have made important contributions to our research projects, and I am also very grateful to them.

Last but not least, I would like to wholeheartedly thank Assoc. Prof. Jan Vykopal, Prof. Herve Debar, and Prof. Youki Kadobayashi, who have been so kind as to review this manuscript. The insightful comments and suggestions they have provided have helped me significantly improve the book.

Contents

Chapter 1
Introduction

Know the small rather than the big, reach the deep rather than the shallow.
Miyamoto Musashi, "The Book of Five Rings," 1645, translated by the author.

This chapter discusses first the motivation for this book, as well as its two-part structure. Then, the main characteristics of the existing literature related to cybersecurity education and training are outlined, followed by a summary of the key contributions the book makes in this respect. The chapter ends with a discussion of the intended audience of the book.

1.1 Background and Motivation

The *Cybersecurity Workforce Study 2023* report published by ISC2, which is the world's leading association for cybersecurity professionals, concluded that the global cybersecurity workforce had an 8.7% year-over-year (YoY) growth compared to the results reported in 2022, to reach approximately 5.5 million professionals [3]. However, it was reported that the workforce gap has increased even more, specifically by 12.6% YoY, to reach a number of almost 4 million professionals that organizations require in addition in order to secure themselves appropriately.

This dire situation is not new, however. Thus, a 2013 report by the National Center of Incident Readiness and Strategy for Cybersecurity in Japan (NISC), formerly known as the Information Security Policy Council, revealed that the existing cybersecurity personnel was insufficient and not well-enough trained. In particular, it was reported that, although there was a total of about 265,000 individuals with cybersecurity-related jobs in Japan at that time, there was also a potential deficiency

R. Beuran, *Cybersecurity Education and Training*,
https://doi.org/10.1007/978-981-96-0555-2_1

of 80,000 such security personnel. Moreover, of the existing cybersecurity personnel, those who actually possessed the required level of skills were considered to be around 105,000, meaning that additional education and training was deemed necessary for the remaining 160,000 individuals [5].

This led to the creation of several cybersecurity education and training programs in Japan that were meant to support the development of future security experts. One such program is CYber Defense Exercise with Recurrence (CYDER), which was created in 2013 by the Ministry of Internal Affairs and Communications (MIC) with the goal of improving the capabilities of local government agencies to cope with cyberattacks. For this purpose, MIC conducted practical cyber defense exercises at several locations throughout Japan until 2015. However, since 2016 CYDER is operated by the National Institute of Information and Communications Technology (NICT), and the scope and frequency of the activities have been extended. Thus, starting from 2018 all the 47 prefectures in Japan are covered, and more than 100 training events are held each year [6].

In addition to the training programs, several endowed chairs were created in Japanese universities to promote cybersecurity education and training activities. One of these endowed chairs was Cyber Range Organization and Design (CROND) that operated at Japan Advanced Institute of Science and Technology (JAIST) from April 2015 to March 2021 with the support of NEC Corporation. The goal of CROND was to advance the field of cybersecurity education and training, especially through conducting research on *cyber ranges*, the network environments that are typically used for hands-on training activities.

As one of the core members of CROND, the author conceived this book as a summary of the knowledge that was created, and the research results that were produced by the endowed chair. Consequently, he hopes it will serve as a helpful guideline for cybersecurity educators and training experts worldwide.

1.2 Book Outline

This book provides a comprehensive overview on cybersecurity education and training methodologies. The book uses a combination of theoretical and practical elements in order to address both the abstract and concrete aspects of the discussed concepts.

The book is structured into two parts. The main focus of the first part of the book is on technical cybersecurity training approaches. Following a general overview on cybersecurity education and training, technical cybersecurity training and the three types of training activities in this context—attack training, forensics training, and defense training—are discussed in detail. In addition, we present specific issues related to the particular case of IoT security training, which has its unique challenges that must be addressed. Lastly, cybersecurity awareness training, also known as end-user training or IT literacy, is also discussed in order to provide a thorough view on cybersecurity education and training methodologies.

The second part of the book describes the main characteristics of cybersecurity training platforms, which are the systems used to conduct the technical cybersecurity training activities. We start by introducing a generic training platform architecture, as well as key elements of the architecture, such as training content and training environments. This is followed by a wide-ranging analysis of actual cybersecurity training platforms, with focus on various CTF[1] systems and cyber ranges that are currently being used worldwide. To better illustrate the concepts discussed in the book, a detailed study of an open-source cybersecurity training platform is also included, namely the integrated cybersecurity training framework CyTrONE [2]. Finally, a cybersecurity training platform capability assessment methodology is introduced as a way to make it possible for the organizations that want to deploy or develop training platforms to objectively evaluate them.

1.3 Existing Literature

The current literature regarding cybersecurity education and training consists mainly of books that are dedicated to teaching practical low-level cybersecurity skills, such as penetration testing and hacking. One example in this category is *Penetration Testing: A Hands-On Introduction to Hacking* by Weidman [8], who is a penetration tester and security researcher. Another example is *Handbook for CTFers* by Nu1L Team [7], which is one of China's top CTF teams. Yet another example is *Network Security Assessment* by McNab [4]. And many other similar books can be easily found through a simple online search.

While such books are useful from the practical perspective of beginners who want to learn this type of low-level skills, they do not discuss the higher-level principles behind cybersecurity education and training. Therefore, such books lack the information that is required to understand how to organize training activities in an effective manner, and how to develop training content or training platforms in order to meet specific training goals.

A more unique perspective is provided in the book *Cyber Security Education: Principles and Policies* by Austin [1]. This is the closest to our book in terms of subject matter, but its main focus is on cybersecurity education principles seen from a mostly theoretical angle. In contrast, our book also discusses practical aspects related to training, thus providing a more concrete view on the topic, as well as readily applicable information that readers can use to plan and conduct various forms of training activities.

[1] CTF (Capture The Flag) is a type of cybersecurity competition in which participants are faced with a number of challenges in which they need to retrieve pieces of information, named "flags," to prove they have managed to solve those challenges.

In addition, the aforementioned book is a contributed one, that gathers the various perspectives of the contributing authors on cybersecurity education. Consequently, the book fails to provide a unified view on cybersecurity education and training similar to the one we present in this book.

1.4 Key Contributions

Based on the above considerations, we conclude that our book fills an important gap in the current literature by taking a middle-ground approach to discussing cybersecurity education and training. Thus, the book provides enough theoretical background and practical details so that it can be used by readers as a comprehensive guideline that makes it possible to effectively address all the issues related to planning and conducting cybersecurity education and training activities.

The key contributions of the present book are summarized below; the corresponding related chapters are also mentioned for reader's convenience:

1. Provides a thorough view on cybersecurity education and training methodologies and tools, focusing on the technical perspective that covers attack, forensics, and defense training (Chaps. 2 through 6).
2. Introduces other specific types of cybersecurity training, such as IoT security training and non-technical awareness training (Chaps. 7 and 8).
3. Discusses a generic cybersecurity training platform architecture, as well as a set of specific CTF and cyber range platforms (Chaps. 9 through 11).
4. Analyzes in detail a case study of an actual cybersecurity training platform, named CyTrONE, emphasizing its features and applicability for particular training activities (Chap. 12).
5. Describes a cybersecurity training platform capability assessment methodology that makes it possible to objectively evaluate training platforms in view of deployment or development (Chap. 13).

1.5 Intended Audience

The intended audience of this book covers the following areas:

- The main audience is cybersecurity education and training practitioners and professionals, both in the academia and industry, who will gain knowledge about how to organize meaningful cybersecurity training activities, and how to practically conduct those activities.
- Another category of potential readers are researchers and postgraduate students working in the area of cybersecurity training, who will gain insights about the current state-of-the-art in this field and will be able to build upon the information presented to extend their research and find new research topics.

- University lecturers and tutors, as well as undergraduate students, will also gain knowledge helping them make better use of the cybersecurity education classes they are tutoring or taking.
- Last but not least, corporate and academic libraries may decide to purchase this book in order to support the cybersecurity education and training activities of the professionals and students in those organizations.

As for the cybersecurity education and training activities that will be discussed, they are mainly related to work roles that have a strong practical component, such as incident responders, system architects, developers, digital forensics investigators, and penetration testers. However, even if the necessary training for certain work roles, such as legal, policy, and compliance officers, is not directly addressed, many of the issues discussed apply to those roles as well, although additional knowledge is required in those cases, e.g., with regard to laws and regulations.

References

1. Austin G (ed) (2020) Cyber security education: principles and policies. Routledge, London
2. Cyber Range Organisation and Design (CROND). CyTrONE GitHub page. https://github.com/crond-jaist/cytrone. Accessed 1 July 2024
3. ISC2 (2023) Cybersecurity workforce study 2023. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf. Accessed 1 July 2024
4. McNab C (2016) Network security assessment, 3rd edn. O'Reilly Media Inc, Sebastopol
5. National Center of Incident Readiness and Strategy for Cybersecurity (NISC), Japan (2013) Cybersecurity strategy. https://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf. Accessed 1 July 2024
6. National Institute of Information and Communications Technology (NICT), Japan. Cyber defense exercise with recurrence (CYDER) (in Japanese). https://cyder.nict.go.jp/. Accessed 1 July 2024
7. Nu1L Team (2022) Handbook for CTFers. Springer, Heidelberg
8. Weidman G (2014) Penetration testing: a hands-on introduction to hacking. No Starch Press, San Francisco

Part I
Cybersecurity Education and Training Methodologies

Part I of the book discusses in detail various aspects related to cybersecurity education and training methodologies. The main focus is on technical cybersecurity training, and the three types of training activities in this context: attack training, forensics training, and defense training. The specificities of IoT security training are also examined, followed by a discussion of cybersecurity awareness training.

Chapter 2
Cybersecurity Education and Training

This chapter discusses first the manner in which we use in this book the concepts of education and training in the context of cybersecurity. Then, an overview of the two main categories of training, technical cybersecurity training and cybersecurity awareness training, is provided, including a discussion of specific issues for each of them. The chapter ends with a comparative analysis of the main characteristics of the two training categories.

2.1 Education Versus Training

The terms education and training are sometimes used interchangeably, especially in relation with cybersecurity, and in this section, we will clarify what are the meanings that we will give to these two concepts in the present book.

2.1.1 Term Connotations

According to the Random House Kernerman Webster's College Dictionary, one definition of *education* is "the act or process of imparting or acquiring general knowledge and of developing the powers of reasoning and judgment." We believe that this is one of the most commonly agreed upon meanings of the word, which equates education with acquiring knowledge, as well as generic reasoning skills.

Another definition given in the same dictionary for the word *education*, however, considers it to be "the result produced by instruction, training, or study." This clearly positions training as one of the methods through which education is achieved.

As for *training*, in the same Random House dictionary, it is defined as "the education, instruction, or discipline of a person or thing that is being trained." Interestingly,

R. Beuran, *Cybersecurity Education and Training*,
https://doi.org/10.1007/978-981-96-0555-2_2

this situates education as a methodology that is used for training, which is the opposite of the connotation mentioned above.

A more accurate definition for the word *training*, in our opinion, is to be found in the Collins English Dictionary, which defines training as "the process of bringing a person, etc., to an agreed standard of proficiency, etc., by practice and instruction," since it emphasizes the important of practice in the context of training.

We can thus say that, in a general context, there is no clear relationship between education and training, and they are sometimes used with very similar meanings. Let us analyze next this issue in the context of cybersecurity.

2.1.2 Education and Training for Cybersecurity

Cybersecurity is one of the fields that requires its practitioners to master both a vast amount of knowledge and a large range of technical skills. For this purpose, cybersecurity education and training programs must first teach the required theoretical knowledge, such as network protocols, operating systems, and cryptography. This must then be complemented with hands-on practice in order to instill the related technical skills: how to use network protocols, how to secure operating systems, how to configure encryption algorithms, etc.

In the book *Cyber Security Education: Principles and Policies*, even though the word education is used in the title, many of the actual book chapters discuss practical aspects as well. For example, several chapters discuss methods for developing cybersecurity skills, such as complementing in-class curricula with experiential activities to apply the learned concepts and skills in real-world settings [1]. We conclude that, in the mentioned book, cybersecurity training is conceived as an intrinsic component of cybersecurity education. However, this begets the question of how to refer to that part of cybersecurity education that is not training.

To simplify the discussion and eliminate the confusion that appears to reign in dictionary definitions and common understanding regarding the relationship between education and training, in this book we will use the term *education* to refer to the act of imparting knowledge, whereas *training* will be used to refer to the use of practice to bring a person to a target level of proficiency.

Since education sciences are already well established, this book will focus mainly on practical aspects related to cybersecurity training. Nevertheless, educational aspects will also be discussed as needed, since many of the cybersecurity training methodologies and platforms include education content, as well as rely on various instructional strategies in order to augment the information retention rate, or to improve trainee motivation, for example.

We note that a challenge in this context is how to design the overall cybersecurity educational program, and the general methodology proposed in [8] is a possible starting point for addressing this issue. Thus, the methodology integrates an educational framework based on institutional, user, and external dimensions, with a set of

pedagogical methods based on learning type, learning level, and informal learning techniques, to provide a thorough but flexible design strategy.

As an indication of the wide variety of approaches that are currently used in the area of cybersecurity education and training, the *Computer Security Education Resource Collection* is a helpful source of information [6]. An important aspect of this collection is that each entry is tagged according to its characteristics, such as "CTF/contest," "curriculum content," "concept framework," or "pedagogical learning objectives," making it easy to determine the type of a resource at a glance.

We also note that, although we can assume that all nations consider cybersecurity capacity building to be of high priority, differences between countries were observed, mainly deriving from differences in economic development and the scale of Internet use [3]. Moreover, countries that had greater and lower levels of maturity in capacity building than expected only on the basis of their development and scale of Internet use were also identified in that study. This signifies that, in the long term, social and cultural differences must also be considered when designing cybersecurity education and training programs.

2.2 Cybersecurity Training Categories

We live in a network-centric society, with most people using IT systems on a regular basis—either in schools, for work, and also after retirement. Thus, ITU estimates that approximately 5.4 billion people, that is 67% of the world population, have used the Internet in 2023 [7]. This means that the current number of regular IT users is really huge. Moreover, they come from various societal backgrounds. Consequently, we can expect that the security-related knowledge and skills of regular IT users are relatively low in general.

The IT infrastructure itself is managed by professionals, who due to the nature of their work must possess at least a medium level of cybersecurity skills in order to be able to carry out their work-related tasks. In addition, a number of security experts make sure that the cybersecurity risks regarding the IT infrastructure are minimized. Such highly skilled experts are also called upon when the need to handle cybersecurity incidents arises.

When considering the need for cybersecurity education and training, it becomes obvious that participant background and skill level are important in determining the most suitable kind of training for a given type of participant. Thus, education and training activities can be broadly divided into two categories:

- Technical cybersecurity training.
- Cybersecurity awareness training.

The relationship that exists between participant type, their skill level, and the corresponding cybersecurity training category is illustrated in Fig. 2.1, and details on each category are provided in the following sections.

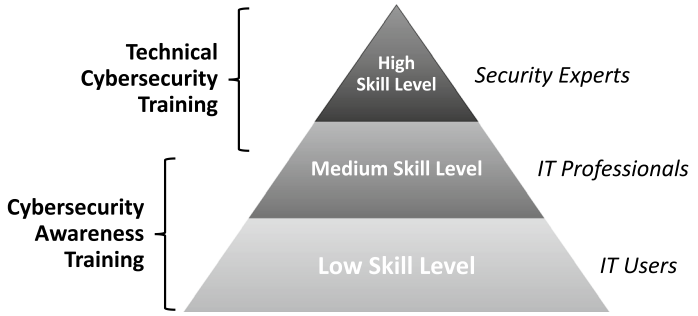

Fig. 2.1 Cybersecurity training approach dependency on participant background and skill level

2.2.1 Technical Cybersecurity Training

We use the term *technical cybersecurity training* to refer to that class of training activities that are aimed at improving the technical knowledge and abilities of high-to-medium skill level participants, such as security experts and IT professionals who are involved in security operations. The goal for this type of training is to make it possible for the trainees to handle efficiently the technical cybersecurity issues that they will encounter in real life.

Since technical security training is aimed at improving the technical skills of the participants, hands-on practice is often included in the training. For this purpose, trainees make use of training environments that are built specifically for cybersecurity training purposes, named cyber ranges. Therefore, conducting training activities is a challenging process, and important preparation is needed on the organizer side. This is the reason why training is not only a service that is provided by academia and commercial companies, but national governments are also getting involved.

For example, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) supports the training and education of the cybersecurity workforce in the U.S. for many categories of personnel: federal employees, critical infrastructure operators, private-sector cybersecurity professionals, as well as the general public. This is achieved by making available a large selection of training exercises, including those that use virtual training environments [11].

From the perspective of an organization that wants to conduct training activities, or even to develop a training platform, it is important to note that the way in which the training environments are configured, and the actual content of the training depend on a series of conditions. These include, for example, issues such as what aspects of cybersecurity training are being targeted, what are the characteristics of target systems, or how motivated the trainees are, as it will be discussed next.

2.2.1.1 Training Aspects

The three aspects or facets of technical cybersecurity training are attack, forensics, and defense [2]. Attack training consists mainly in teaching *ethical hacking* or *penetration testing* (also called *pentesting*) techniques. Different from a malicious attack, pentesting is an authorized simulated cyberattack on an organization network conducted in order to assess the cybersecurity posture of that organization. Forensics training refers to learning the skills needed to investigate the consequences of cyberattacks, so that trainees which can determine relevant information, such as how an attack was started, what mechanisms were used, what assets were affected, and so on. As for defense training, it refers to making the trainees capable of protecting and defending a system from cyberattacks, both via the preliminary steps of securing the system, as well as by responding to an actual live attack.

We note that learning how to pentest also helps with the development of forensics skills. In addition, by leveraging the perspective of pentesters, trainees can deeply understand the practical mechanisms of cyberattacks—a steppingstone that makes it possible to later design and build defense mechanisms. It can be said, therefore, that pentesting training is an entry point for cybersecurity training, and this is the reason why security experts often start training via such activities.

A similar vision is shared by the author of *Network Security Assessment*, Chris McNab, who states that the best way to find out how to secure a network is "to attack it, using the same tactics attackers employ to identify and exploit weaknesses." The author proceeds then to demonstrate common security vulnerabilities, and the steps used to identify them by describing a methodology for performing network-based penetration testing in a structured manner [9].

More details about technical cybersecurity training will be provided in Chap. 3, with each specific training aspect being detailed in Chaps. 4 through 6.

2.2.1.2 Target System Characteristics

Technical cybersecurity training is usually conducted in relation with typical computer networks. In this case, the creation of the appropriate training environments is relatively straightforward in terms of the technologies to be used.

However, the advent of the Internet of Things (IoT) has led to a significant rise in security incidents related to IoT networks and technologies. Given that IoT devices and protocols have different characteristics compared to regular computers and network protocols, such as lack of displays, lower processing capabilities, and simplified features, creating an IoT security training platform poses different challenges. Consequently, such platforms need to consider the specificities of IoT systems, and new training methodologies and content must be developed.

Given the many issues related to IoT security training and the importance of the topic in the wider field of technical cybersecurity training, we will discuss in detail the methodologies for IoT security training in Chap. 7.

2.2.1.3 Trainee Motivation

Given that the target of technical cybersecurity training are mainly IT professionals who want to improve their skills, it is assumed, in general, that they are highly motivated to take part in the training activity. Consequently, instructors create the training content by focusing on the technical elements that are required to help participants acquire the desired skills.

However, not all trainees are equally motivated, and participants to some technical cybersecurity training programs can be young people who have just started taking an interest in cybersecurity. Therefore, in order to increase the motivation of such trainees, educators may create training content that balances the technical elements with other elements that will make it more fun to take part in the training activity. This is because motivated trainees are more willing to actively participate in the training, and also to return for future training activities.

A typical example in this context is the case of Capture The Flag (CTF) competitions. In CTFs, the technical aspects are split into small, focused tasks, and score tables and badges are introduced to keep the participants interested and motivated. The CTF type of training was popularized by the annual DEF CON cybersecurity conference, where it was first introduced in 1996 [5], but CTF events are currently being held in most countries and for a wide range of participants, including starting at elementary school level in some cases.

It is, therefore, obvious that the way in which the training content for technical cybersecurity training is created and how it is presented plays an important role in increasing trainee motivation. The various challenges regarding content creation will be discussed in more detail in Chap. 9, in particular in Sect. 9.2.

2.2.2 Cybersecurity Awareness Training

The wide public of regular IT users, as well as those IT professionals who do not require security skills, are not in need of technical cybersecurity knowledge and skills. Instead, they must acquire basic knowledge about IT and security, which is sometimes called *IT security literacy* to emphasize its importance in the modern society. Such knowledge and skills enable IT users to handle correctly any cybersecurity issues they may encounter during their typical use of IT technology.

Given how wide the public to which this type of education is addressed is, national governments have taken steps to ensure that such training takes place at the needed scale and with the necessary scope for it to be effective. For example, the U.S. Congress has introduced in 2021 the *American Cybersecurity Literacy Act*, which requires the administration to develop and conduct a cybersecurity literacy campaign with the goal of increasing the knowledge and awareness of the best practices needed to reduce cybersecurity risks [10].

In this book, we will use the term *cybersecurity awareness training* to refer to that class of training activities that focus on providing the basic knowledge and

abilities to medium-to-low skill level participants, such as regular IT users and those IT professionals that are not directly involved in security tasks. The goal of this type of training is to minimize the cybersecurity risks that the trainees will have to face during their daily life and work activities.

Given the difference in training methodology and target learners compared to technical cybersecurity training, cybersecurity awareness training faces additional challenges in regard to training content creation and trainee motivation.

2.2.2.1 Training Content Creation

Typically, the content of cybersecurity awareness training courses is created manually by educators, who try to include materials about all the areas of knowledge that they consider the training should cover. The creation is, therefore, a time-consuming process that also leads to the possibility of having outdated content. This can happen, for example, due to the evolution of security concepts, the appearance of new security issues, and so on. In particular, the fact that manually created training content is potentially updated only rarely can become a serious issue in the quickly evolving field of cybersecurity.

Automating the creation of training content is a potential solution for this issue. For example, Natural Language Generation (NLG) techniques could be employed to automatically generate the training content based on various knowledge bases, such as publicly available data from Wikipedia. Such automatic generation comes with several challenges about the quality of the generated training content. However, these challenges can be addressed by leveraging the recent advances in the NLG field, such as Large Language Models (LLMs).

2.2.2.2 Trainee Motivation

We have mentioned already that trainee motivation issues can occur for technical cybersecurity training. However, regular IT users are typically even less motivated than technical personnel when conducting training. This is because cybersecurity awareness training courses can be perceived as an unnecessary burden added to the normal work tasks of the trainees, especially when taking the courses is mandated by their organization.

Various approaches can be used to make the training activity more attractive and effective, and one such possibility is the *serious game* approach. Serious games are a type of games that incorporate pedagogic elements, and that are not intended to be played primarily for amusement purposes. Whereas the concept of serious games has been initially introduced in the context of role-playing in the 1970s [4], it has been since extended to computer games as well. By using the process called *gamification* to incorporate game elements into cybersecurity awareness training, it becomes possible to increase the motivation of the learners; improvements in the retention rate are also to be expected.

Moreover, the automatic content generation mentioned above also makes it possible to create training content that is more attractive than the manually generated one. For example, game-like components, such as crossword puzzles, can be introduced into the training as an addition to or replacement of the typical quizzes that are used in IT literacy training. Consequently, automatic training content generation as well has the potential of making the overall cybersecurity awareness training process more enjoyable.

More details about cybersecurity awareness training methodologies, including specific approaches for increasing trainee motivation, will be provided in Chap. 8, where a related case study will also be discussed.

2.2.3 Training Category Comparison

Before proceeding to the in-depth discussion in subsequent chapters of the various aspects related to technical cybersecurity training and cybersecurity awareness training, we will compare here the fundamental properties of these two methodologies. Table 2.1 summarizes this comparison, which we conducted from several perspectives, as follows:

- Target audience: Who is the training addressed to?
- Training method: How is the training conducted?
- Main challenge: The most significant issue regarding that training category.

2.2.3.1 Target Audience

Regarding the target audience of the two types of training, while security experts and regular IT users are the obvious targets for technical cybersecurity training and

Table 2.1 Comparison of technical cybersecurity training and cybersecurity awareness training

Feature	Technical training	Awareness training
Target audience	Security experts, IT professionals with security involvement	Regular IT users, IT professionals without security involvement
Training method	Hands-on training that is conducted either on-site or online	E-learning (with quizzes), video training, reading materials, etc.
Main challenge	Create technical content suited for the participants to learn the target skills	Ensure that participants are motivated and can apply the knowledge in real life

cybersecurity awareness training, respectively, IT professionals can benefit of both types of training, depending on what is the scope of their work.

On the one hand, those IT professionals who are also involved with security issues, as it often happens in smaller companies, for example, should make sure to take technical cybersecurity training courses. On the other hand, those IT professionals who have no security involvement, as it may happen in larger companies, where the separation of professional roles is stronger, can limit themselves to taking cybersecurity awareness training courses only, even though they could also benefit from technical training.

2.2.3.2 Training Method

Technical cybersecurity training focuses on teaching skills; hence, it is conducted via hands-on activities in which participants can exercise their existing skills and learn new ones via solving practical problems. These hands-on activities can be conducted on-site, in which case the educators and staff can be involved more closely in the training process, assisting the participants as needed. Alternatively, the hands-on activities can also be conducted online when the focus is more on self-learning via the tasks included in the training.

Currently, cybersecurity awareness training is often conducted via e-learning methods that typically include quizzes to evaluate participants' knowledge and to determine if they have achieved a passing score or need to repeat the training. However, video training or even just reading materials are also used sometimes, which was the initial manner in which cybersecurity awareness training was conducted. Moreover, such training methods are easier to manage and deliver. Nevertheless, this type of passive activities has a lower engagement of the participants and does not allow for evaluating their knowledge.

2.2.3.3 Main Challenge

Each training category has its own specific challenges that we will discuss in more detail in the following chapters. For the purpose of this comparison, however, we will focus on what we consider to be the main challenge instructors are faced with in each case.

Thus, for the case of technical cybersecurity training, content creation is the biggest challenge from our point of view due to two main issues. First of all, the complexity of the technical training content hinders automation, and content creation itself is done manually by educators/instructors; hence, it is a tedious process that requires creators to master a significant amount of knowledge and skills. Furthermore, malware and security threats evolve rapidly, meaning that new content needs to be created relatively frequently in order to be able to train additional skills that are applicable to current security issues.

As for cybersecurity awareness training, content creation typically requires simply writing explanation text and creating visual aids, hence no technical knowledge is required. This also means that content can be updated, if needed, with relatively less effort. Moreover, automated content generation techniques can be used to create and update the content with limited human intervention. However, while security experts are usually motivated to learn new skills, regular IT users often perceive awareness training as uninteresting, especially if it is a work-mandated type of training. Therefore, we consider that the main challenge in the case of cybersecurity awareness training is to create such training content and organize such training activities that keep the participants interested and motivated. In addition, the new knowledge that is gained via the training activity must be structured in such a manner that it is readily applicable to practical situations.

References

1. Austin G (ed) (2020) Cyber security education: principles and policies. Routledge, London
2. Beuran R, Chinen K, Tan Y, Shinoda Y (2016) Towards effective cybersecurity education and training. Tech. Rep. IS-RR-2016-003, Japan Advanced Institute of Science and Technology
3. Creese S, Dutton WH, Esteve-González P (2021) The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. Pers Ubiq Comput 25(5):941–955. https://doi.org/10.1007/s00779-021-01569-6
4. Cruz-Cunha MM (2012) Handbook of research on serious games as educational. Business and research tools. IGI Global, Hershey
5. DEF CON Cybersecurity Conference: DEF CON website. https://defcon.org/. Accessed 1 July 2024
6. Denning T (2024) Computer security education resource collection. https://securityeducationresourcecollection.net/. Accessed 1 July 2024
7. International Telecommunication Union, Telecommunication Development Sector (ITU-D): ITU-D ICT statistics. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. Accessed 1 July 2024
8. Kim E, Beuran R (2018) On designing a cybersecurity educational program for higher education. In: Proceedings of the 10th international conference on education technology and computers, pp 195–200. https://doi.org/10.1145/3290511.3290524
9. McNab C (2016) Network security assessment, 3rd edn. O'Reilly Media Inc, Sebastopol
10. U.S. Congress: American cybersecurity literacy act. https://www.congress.gov/bill/117th-congress/house-bill/4055. Accessed 1 July 2024
11. U.S. Cybersecurity and Infrastructure Security Agency (CISA): Cybersecurity training & exercises. https://www.cisa.gov/cybersecurity-training-exercises. Accessed 1 July 2024