Towards Effective Cybersecurity Education and Training

Razvan Beuran, Ken-ichi Chinen, Yasuo Tan, Yoichi Shinoda

School of Information Science
Japan Advanced Institute of Science and Technology

October 14, 2016

IS-RR-2016-003

Towards Effective Cybersecurity Education and Training

Razvan Beuran, Ken-ichi Chinen, Yasuo Tan, Yoichi Shinoda
Japan Advanced Institute of Science and Technology

Abstract

Effective cybersecurity education and training are important for preparing current and future IT professionals to properly and swiftly deal with real-life security incidents. In this paper we use the main cybersecurity training programs in Japan as a detailed case study for analyzing the best practices and methodologies in the field of cybersecurity education and training. Based on this analysis and our first-hand experience with some of the said training programs, we then define the requirements that must be met in order to ensure effective cybersecurity education and training. Finally, we discuss our research and development endeavor towards creating a framework that meets these requirements, so as to facilitate effective education and training in cybersecurity.

Keywords: Network security; cybersecurity education; cybersecurity training; cyber range.

1 Introduction

According to a 2013 report by the National Center of Incident Readiness and Strategy for Cybersecurity in Japan (NISC) [7], cybersecurity personnel is not trained well enough and is insufficient. Thus, from a total of about 265,000 persons with cybersecurity-related jobs in Japan, it was considered that about 160,000 of them require supplementary training; moreover, it was deemed that about 80,000 additional personnel was needed [8].

As a consequence, several cybersecurity education and training programs have been created in Japan, such as enPiT-Security (SecCap), CYDER, or the Hardening Project, that focus on practical activities for participants with different skill levels, such as university students or IT professionals. These programs are little known outside Japan, and to the best of our knowledge this paper is the first to introduce and analyze them in English language.

The training programs in Japan will be used as a case study for a detailed analysis of the best practices and methodologies in cybersecurity training. This analysis and our first-hand experience with security training at the Japan Advanced Institute of Science and Technology (JAIST) are then employed as the basis for defining a set of requirements that must be met in order to ensure the effectiveness of cybersecurity education and training. This work is done within the framework of Cyber Range Organization and Design (CROND), an NEC Corporation endowed chair established at JAIST in April 2015 with the goal of advancing the field of cybersecurity education and training.

The main contributions of this paper are as follows:

- We introduce the main cybersecurity training programs in Japan, several of which we are directly involved with (Section 2);
- We analyze the current best practices and methodologies for cybersecurity training, and define requirements for ensuring the effectiveness of such activities (Section 3);
- We outline the R&D efforts of the CROND chair at JAIST towards effective cybersecurity education and training (Section 4).

The paper ends with conclusions, acknowledgments, and references.

2 Cybersecurity Training in Japan

In this section we shall describe the main cybersecurity education and training programs available in Japan, which we believe are mostly unknown outside the country. These training programs will become the basis of our analysis of cybersecurity training methodologies that will be presented in Section 3. We exclude from our presentation those cybersecurity training programs in Japan that are not publicly available, such as internal company training programs, etc.

2.1 Secure Eggs

Secure Eggs is a basic hands-on cybersecurity course offered by Nomura Research Institute (NRI) SecureTechnologies [11]. The word *Eggs* in the program title, which is an acronym for "Essentials and Global Guidance for Security", emphasizes the program's focus on basic cybersecurity skills. There are two course categories in the Secure Eggs program, as follows [10]:

- *Basic course*: A two-day hands-on course on fundamentals of IT and cybersecurity;
- *Practical courses*: One-day specialized hands-on introductory courses focusing on topics such as web application security, forensics, and incident response.

The aim of these courses is to provide the knowledge and skills necessary at entry level for jobs such as penetration testing, forensics analysis or incident handling. The courses are paid, and they are organized three times a year for the basic course, and twice a year for the specialized courses.

We mention that NRI SecureTechnologies also provides advanced third-party courses, such as those offered by the SANS Institute in the U.S.A., as well as CISSP certification. Some of these will be discussed in Section 2.5.

2.2 enPiT-Security (SecCap)

The enPiT-Security training program (also known as SecCap) [4] was started in April 2013 by a consortium of five Japanese universities, including JAIST. The other consortium members are: Tohoku University, Nara Institute of Science and Technology, Keio University, and Institute of Information Security.

The SecCap program is aimed at university students, with the goal of developing the basic skills needed by IT security engineers through courses and hands-on activities regarding security-related aspects of operating systems, software, networks, as well as malware-related countermeasures and technologies.

The program participants are students at the end of their studies in the five participating universities, selected based on their cybersecurity knowledge and interests. The program curriculum and training content are decided in common by the five consortium members, by drawing on their corresponding cybersecurity-related courses. Various courses and twelve practical sessions are held during each academic year, with an intensive training camp held once a year.

2.3 CYDER

CYDER (CYber Defense Exercise with Recurrence) is a training program initiated in September 2013 by the Ministry of Internal Affairs and Communications in Japan [6]. The program focuses on the improvement of the competence in dealing with cyberattacks of the IT and cybersecurity-related personnel of central government offices, independent administrative agencies, as well as large companies.

The practical cybersecurity training conducted in the CYDER program takes place over two days, based on a training scenario defined by several organizing parties, including JAIST members. Throughout the program there is a focus on the use of hands-on training, so that the trainees become able to handle potential cybersecurity incidents in real life. Thus, the training activity has two key elements:

- Performing an analysis of a cyberattack, which is recreated during the training based on details from actual past security incidents;
- Considering a defense model for the given cyberattack, including incident reporting and outsourcing of the detailed forensics investigation.

The CYDER program holds 6-7 training sessions per year, with a total number of over 200 participants. Attendance is done on a team basis, with 3-4 members per team who are all part of the IT personnel of the same organization.

Starting in the fiscal year 2015, a one-day version of the CYDER program was created, named CYDER Lite, which aims to lower the entry barrier to the program by reducing the amount of technical skills required to complete the training, while still providing the basic knowledge regarding cyberattack analysis and defense. Only two sessions of CYDER Lite were held in 2015, however the number will be increased to about ten sessions per year starting in 2016.

2.4 Hardening Project

The Hardening Project is a two-day training event organized by the Web Application Security (WAS) Forum starting in 2012 [16], and includes JAIST members as part of the organizing committee. This cybersecurity activity held twice a year has as goal maximizing the strength of the defensive cybersecurity techniques of its participants.

Attendees are divided by organizers into teams before the competition, based on their self-declared skills. On the first day of the event, called *Hardening*, the teams compete in terms of the security hardening they can provide to a virtual e-commerce website created for the purpose of the event. The winning team is decided based on the amount of virtual sales their website generated during the duration of the competition, as an objective and realistic measure of the overall effectiveness of the hardening.

The training conducted by the Hardening Project has a very realistic scenario, that could easily be encountered in real life. Thus, participants are tasked with actually dealing with security incidents and patching vulnerabilities of the e-commerce website, all skills that are readily applicable to real-life situations.

For this purpose, the Hardening Project hands-on activities are conducted on an emulated environment built on the large-scale network experiment testbed StarBED [9]. The emulated environment is realistic in terms of it composition and content, with more than a dozen servers (running as virtual machines on the physical StarBED hosts) allocated to each team, and an architecture mimicking typical e-commerce sites.

The second day of the Hardening Project event, called *Softening*, is education oriented, with the organizers providing feedback to participants regarding the previous day activities, so that they can fill in whatever knowledge and ability gaps they may have had.

Since 2015 a shorter version of the training program, called "MINI Hardening Project", is being organized once a year. This event has similar rules with the main training activity, however instead of a full day, the competition duration is of only 3 hours, hence it is a more intense and focused event.

2.5 Other Training Programs

In addition to the programs that we have described so far, several other cybersecurity training and education events take place in Japan, for instance in the form of mini security camps. The main training methodology used in these events is the Capture The Flag (CTF) type of competition. Participation to these programs is either individual or team based, and rules are similar to those of CTFs that take place elsewhere in the world.

The most famous CTF in Japan is SECCON (Security Contest) [5], which takes place eight times a year in various locations in Japan, and is a qualifying competition for DEF CON [1]. In addition to the main contest, sessions called "CTF for Beginners" were introduced in 2014, that lower the entry barrier by focusing on basic cybersecurity techniques. CTF for Beginners is also held eight times a year.

The SANS NetWars program [13], made available in Japan through NRI SecureTechnologies, is a thorough cybersecurity training program, that includes both hands-on courses and exercises in a training environment, including through online access. SANS NetWars training activities are mostly based on the CTF concept.

3 Training Methodology Analysis

As part of the mission of the Cyber Range Organization and Design (CROND) chair at JAIST to provide guidelines on the design and architecture of cyber ranges, and create material for cybersecurity training and education, we have conducted a systematic analysis of the best practices and methodologies used in cybersecurity training.

3.1 Cybersecurity Training Taxonomy

Our taxonomy of methodologies used in cybersecurity training focuses on two main aspects: (i) the content of the training programs, and (ii) the approaches taken for conducting the associated hands-on activities. In addition, several other features are used in order to provide a more thorough view on the characteristics of each program.

3.1.1 Training Content

Real-world security incidents typically start with the exploitation of a software vulnerability, which represents the attack vector of the incident. Once an attack is detected, it is analyzed in detail to ensure that its mechanisms are well understood. During the incident response, the vulnerability needs to be patched, so that it cannot be further exploited.

This incident pattern leads to three main categories of cybersecurity training:

Attack-oriented training Provides the experience of recreating vulnerability exploitation techniques, and includes activities such as penetration testing, which make use of the same tools and methodologies that attackers employ.

Defense-oriented training Focuses on the design and implementation of vulnerability protection mechanisms, so as to prevent similar future attacks.

Analysis/forensics-oriented training Aims to cultivate a deeper understanding of the phenomena related to vulnerability exploitation and patching, including the identification of targeted attack campaigns, and so on.

The three categories of training mentioned above are not mutually exclusive, and it is only through their combination that cybersecurity personnel can achieve the state of *readiness* needed to effectively handle security incidents in a timely manner. The relationship between the phases of real-world cybersecurity incidents and the categories of training activities based on their content is depicted in Figure 1.

3.1.2 Training Activities

Another perspective on cybersecurity training can be had by focusing on the approach taken for the practical training activities, which mainly depends on the kind of skills a given training program aims to develop.

We consider that security-related skills can be divided into three main classes:

- *Individual skills:* Standalone cybersecurity techniques, such as network sniffing, vulnerability scanning, password cracking, etc.;

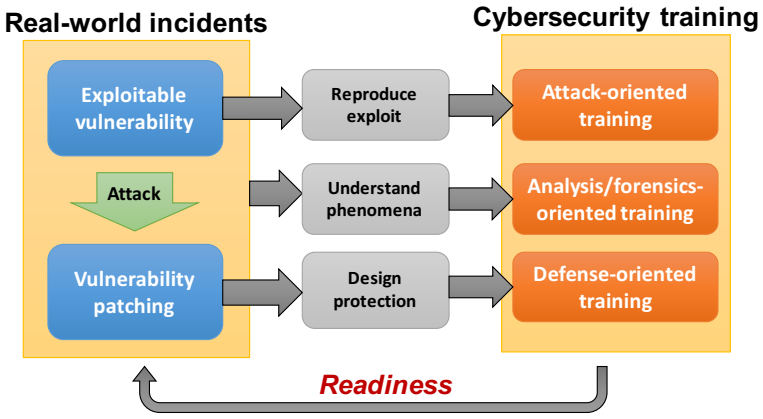

Figure 1: The relationship between real-world cybersecurity incident phases and training categories based on their content.

- *Team skills:* Abilities needed for a cybersecurity team to be effective as a whole, such as cooperation and communication;
- *CSIRT skills:* More advanced team skills needed for the adequate operation of a CSIRT (Computer Security Incident Response Team), such as the ability to put external resources to use, to handle attack escalation, to manage the supply chain, etc.

Let us analyze the methodologies used in cybersecurity training, contingent upon the skills that are targeted in a given training activity. For developing or testing individual skills, simple problem/question-based training is sufficient, however more complex and realistic scenarios are needed for team skill training. This leads to the need of a continuous practical scenario for training CSIRT skills, which is the most realistic case.

Depending on the training methodology, the environments used in cybersecurity training can range from desktop-based training (which is the most often used training environment), to simplified virtual machine (VM)-based environments for most of the individual skills. More complex skills require more elaborate network environments, including the use of emulated environments that reproduce actual computer settings and network topology in detail. As the realism of the training environment increases, the effectiveness of the training will also increase, as the trainees are placed in situations similar to real-world incidents, hence the skills they develop will be readily applicable to real-life conditions.

Increasing the complexity of the training environment naturally leads to cost increases, as equipment and environment setup costs become larger. This is the reason why most training is being done on desktops, and only advanced training is conducted in complex environments. As a side comment, training environment setup currently requires advanced security knowledge and a significant amount of manual configuration; this leads to the fact that for really complex training environments the setup cost exceeds by far the equipment cost.

Figure 2 summarizes our discussion regarding the appropriate cybersecurity training methodologies for developing given target skills, and the corresponding

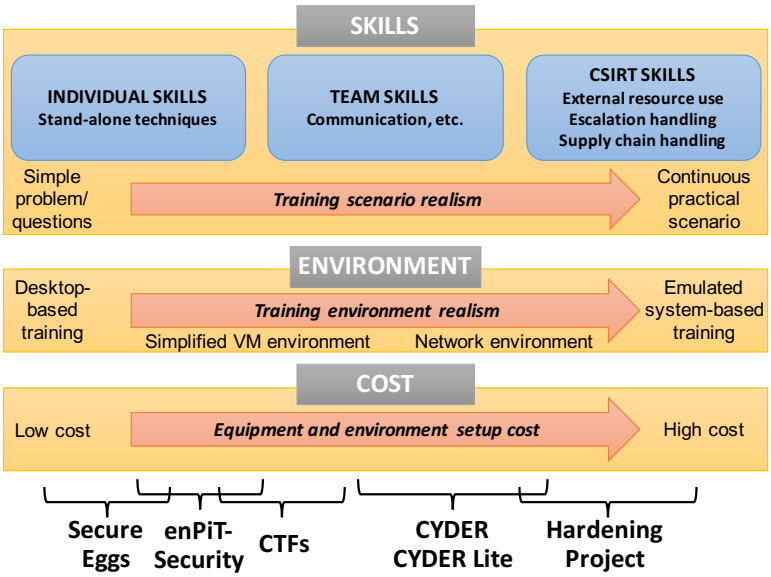

Figure 2: The relationship between various aspects of cybersecurity training activities: target skills, training methodologies, environment complexity, and cost.

training environment complexity and cost.

3.1.3 Other Features

In addition to content type and hands-on activities, we also consider the following characteristics important in order to fully define a certain cybersecurity training program:

Participants The target participants of a certain training program, hence those who can benefit from it, such as students or professionals.

Level The expected ability level of the target participants, such as beginner, medium, advanced (in this paper we discuss technical training, so we assume the participants have a Computer Science background).

Availability Whether participation to a training program is free or not, hence whether there is any financial barrier to entry.

Frequency The frequency per year with which training sessions (events) of a given program are held, therefore how many opportunities participants have for taking that program.

3.2 Comparative Analysis

In this section we shall perform a comparative analysis of the main cybersecurity training programs in Japan, first from the point of view of their content and features, and then from the point of view of the hands-on activities conducted.

Program Name	**Content**	**Skills**	**Participants**	**Level**	**Availability**	**Frequency**
Secure Eggs	All types	Individual	Professionals	Beginner	Paid	5 events / year
enPiT-Security	All types	Individual/team	Students	Beginner	Free	1 event / year
CYDER	Analysis	Team/CSIRT	Professionals	Medium	Free	8 events / year
Hardening Project	Defense	Team/CSIRT	Anyone	Any	Free	3 events/ year
CTFs	Attack	Individual/team	Anyone	Advanced	Free/paid	$>$ 20 events / year

Table 1: Comparison of the main cybersecurity training programs in Japan in terms of their content, target skills, and other features (target participants, expected ability level, availability, and frequency).

3.2.1 Program Content and Features

The characteristics of each of the training programs discussed in Section 2 are presented in Table 1.

Introductory training programs, such as Secure Eggs and enPiT-Security have a broad training focus, hence all the training content categories are included, albeit not in much detail. The more advanced programs are typically more specialized, such as CYDER on analysis and forensics, the Hardening Project on defense, and CTFs on attack-oriented training, although elements of other training content categories are included in most cases.

In terms of target skills, Secure Eggs and enPiT-Security mainly focus on individual skills, with elements of team skills for the latter. CYDER and Hardening Project have a definite focus on team skills, including elements of CSIRT. CTFs are usually about individual skills for contests with individual participation, but can include rudiments of team skills for contests with team-based participation. For a discussion of how the target skills influence the hands-on activities of a training program, please refer to Section 3.2.2.

If we consider the target participants, our data indicates that although there are several programs aimed at professionals, there are also programs aimed at students, and programs for which affiliation does not matter. This is very important for non-professionals for two reasons: (i) They have various opportunities to train in cybersecurity areas, even though they may still be students; (ii) They can take part into the same programs as the professionals, and learn directly from them (e.g., by becoming members of the same team, as is the case of the Hardening Project).

Regarding the expected (prerequisite) ability level of the participants, again we can see that programs vary from beginner level all the way to advanced one, and in some case the cybersecurity skill level is not important *per se*. In such cases it is assumed that participants have other skills (e.g., communication) that make them valuable team members; the best example of such heterogeneous teams is again the Hardening Project. CTFs typically require a advanced skills to begin with, hence they are more oriented towards skill testing rather than learning.

Most of the training programs that we have described in this paper are free, being sponsored by government organizations, universities, and so on. Paid programs are of course available as well, but the fact that free cybersecurity training programs are available for any kind of participants with any ability level considerably lowers the barrier to entry for attending such training. This purposeful policy is expected to significantly increase the skill level of IT and security professionals in Japan. However, we would like to stress in this context that, while paid program usually make no selection of the candidates, in the free programs the trainees may need to be selected from the candidates based on various criteria, such as affiliation, job position, motivation to attend the training, etc.

The frequency of the training sessions (events) of a training program depends significantly on the program type. The enPiT-Security program takes place during an academic year, so in principle a student has only 1 opportunity to attend the program. The Hardening Project has 2 sessions per year, plus an additional MINI session, hence 3 events in total. On the other hand, Secure Eggs, which is a paid program, provides 3 general and 2 specialized sessions per

year, and more sessions can be arranged on demand. Among the free programs, CYDER is the one with the largest number of sessions per year, especially if the CYDER Lite sessions are included, for a total of 8 events currently. CTFs also have multiple sessions every year if we include all programs; to take the case of SECCON, 8 advanced and 8 beginner sessions are available per year, plus 2 sessions dedicated to female participants.

3.2.2 Hands-on Activities

Next we shall focus on the practical activities that are part of the cybersecurity training programs in Japan, and on how this relates to the required training environments and the training cost (independently on the cost actually charged to participants).

For the purpose of this analysis please refer again to Figure 1, specifically the bottom part, which displays information about the cybersecurity training programs discussed so far. The placement of each training program on the horizontal axis was decided depending on the three analysis criteria that we have mentioned in Section 3.1.2, namely (i) skills that are to be developed, (ii) environment complexity, and (iii) training cost. This evaluation was made based on our first-hand experience with several of these programs and/or feedback from the organizers. Note the overlap of the coverage of the training programs in terms of these characteristics, meaning that the programs' feature sets are not disjoint.

In left-to-right order at the bottom of Figure 1 we have first of all Secure Eggs, which is the most basic of the presented programs in term of methodology and target skills, followed by the enPiT-Security program, which uses somewhat more complex training scenarios. For these programs the associated training environment complexity and realism are low, hence setup costs are also low.

To the left of these programs in the bottom area of the figure we have placed the CTF-type competitions, which target not only individual skills but also team skills, and have more variation in the training conditions and environments, hence require more complex and costly setups.

In the middle and right side at the bottom of Figure 1 are located the CYDER and CYDER Lite programs, which use realistic albeit simplified scenarios for training, and which require team-based participation. Finally, the most realistic training program in our analysis is Hardening Project, which uses complex training environments (at a high setup cost), and teams with membership decided by the organizers.

3.3 Training Effectiveness

Based on the training program taxonomy and comparative analysis that we have presented so far, we now define a series of requirements that must be met in order to ensure the effectiveness of cybersecurity education and training. Thus, in order for a program to be effective, the following conditions must be satisfied:

- The training content should be appropriate for the target audience in terms of knowledge and ability levels;
- The training content should be in accordance with the skills that the program aims to develop;

- The training program should use hands-on activities for developing practical abilities, so as to ensure that trainees can subsequently deal with real-life incidents;
- The training program should reach as large an audience as possible, in order to have a significant impact on the cybersecurity readiness of a country;
- The training program should have good cost/performance characteristics, so that it sustainable on long term.

To discuss how such requirements can be met in practice, we note that the effective training requirements given above refer to two key aspects: (i) training content, and (ii) hands-on activities. Therefore, in terms of practical implementation, the above requirements can be converted into two necessary features for any effective cybersecurity education and training platform:

1. Ability to easily modify the training content and add new one;
2. Ability to automatically create and manage the training environment.

The first implementation requirement, easy modification and addition of training content, addresses the need for content that is appropriate to the training audience and target skills. Such an ability would solve an issue many current training programs have: training content (description, question text and answers, etc.) is statically defined in the beginning. Therefore, the training organizers of a particular event cannot adapt the content to match actual event circumstances, such as trainee background and level, or to simply add some variation, nor can they add new content, for instance to address emergent security issues, etc.

The second implementation requirement, automatic creation and management of the training environment, addresses the need for hands-on training activities organized and conducted in a scalable and cost-effective manner. This ability deals with the other significant issue of all the training programs we know of: the training environment is always set up by experts, either manually or by using custom/proprietary tools. This impacts on the scalability of the program, hence its ability to address large audiences, and also leads to poor cost/performance characteristics.

In Section 4.1 below, we'll discuss how we address these requirements in our R&D activity at JAIST.

4 Cyber Range Organization and Design

Cyber ranges, virtual environments used in cybersecurity training, are often used for hands-on training activities, since practical experience and skills are essential for effectively handling security incidents. The Cyber Range Organization and Design (CROND) chair was created at JAIST in April 2015 with a twofold mission:

1. Study the architecture and develop mechanisms for the creation of cyber ranges, so as to improve the effectiveness of cybersecurity training for a large number of participants;

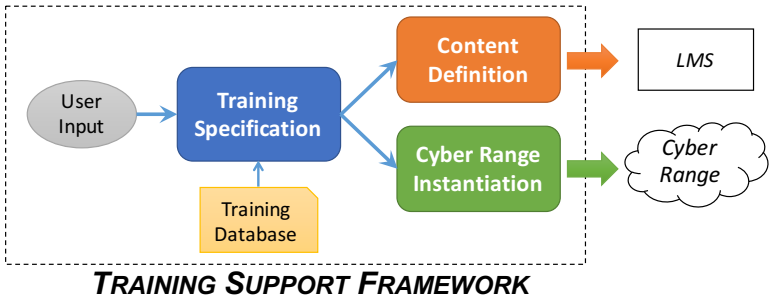

Figure 3: Architecture of the cybersecurity training support framework developed by CROND.

2. Design the related educational programs and teaching materials for cybersecurity training activities.

In the next sections we shall describe two of our projects in this context.

4.1 Training Support Framework

At CROND we designed and started implementing a training support framework that meets both practical requirements discussed in Section 3.3. Thus, based on organizer input and a training database, our framework automatically defines the content and instantiates the cyber range that correspond to the given activity, while requiring only a limited amount of technical knowledge from the part of the training organizers.

The architecture of the training support framework that we are currently implementing is shown in Figure 3. Its main components are described below:

Training Specification Based on user input and a training database (including training scenarios, previous security incident and vulnerability information, etc.), this module produces a *content description* and the associated *cyber range description* that fully define the corresponding training activity.

Content Definition Based on the content description, this module generates the training content in an appropriate format, for instance to use in an LMS (Learning Management System) such as Moodle [2], which serves as the training user interface.

Cyber Range Instantiation Based on the cyber range description, this module automatically creates the corresponding cyber range in an actual computer and network environment, such as StarBED [9].

Training scenarios (descriptions, questions and answers) are represented in our framework as text files in YAML format, therefore they can be easily updated by the training organizers, without a need for significant technical knowledge. Moreover, we envisage that in the future questions could also be partially generated based on meta-level descriptions, such as training topics, by using

information from the training database. In both cases, the corresponding training content as shown to trainees is produced automatically, thus meeting the first implementation requirement regarding the easy modification and addition of training content.

As mentioned before, currently cyber ranges are highly customized, and their setup requires a high level of cybersecurity expertise. This makes it prohibitive to setup complex environments, which leads to high training costs. The reuse of cyber range environments for subsequent training sessions is often considered an acceptable solution, however this limits the quality of the training, since the environments cannot be updated if the need arises. Moreover, it engenders the possibility of information leakage, hence it decreases the effectiveness of the cyber range as a skill-evaluation tool.

The automatic cyber range instantiation functionality in our framework addresses this issue, and thus meets the second implementation requirement for effective cybersecurity education and training, the automatic creation and management of the training environment.

Although the implementation of the overall training support framework is currently ongoing, the core component of the system, the Cyber Range Instantiation module is practically finalized; its design and implementation are presented in [12]. We plan to make this component public at the end of fiscal year 2016, including a series of security-specific modules, such as cyberattack emulation, dummy malware, etc. The entire training support framework, including sample training content for various audiences, will be made public at the end of fiscal year 2017.

We outline below some of the advantages and possible uses of our training support framework:

- Bridge the gap between descriptions of training content (such as the NIST "Technical Guide to Information Security Testing and Assessment" [14]), and the environment in which the corresponding training activities should occur;

- Provide flexibility in creating cyber ranges and updating their content based on information regarding recent security incidents, the skill level of the participants, etc. Consequently, improve the effectiveness of the training through ensuring a higher variability of the scenarios;

- Decrease the cost of setting up complex training environments, and thus improve the scalability of cybersecurity training, through allowing for a large number of training sessions and participants.

Although automatic generation has been explored before in the context of cybersecurity training, it was reduced in scope, e.g., to CTF problem generation to limit flag sharing [3]. To the best of our knowledge, our training support framework that includes automatic cyber range creation will be the first open-source framework of its complexity, and through its advanced features we hope it will significantly contribute to advancing cybersecurity training and education worldwide.

4.2 Cybersecurity Literacy

People have become more and more reliant on the Internet, which is leading us to a world in which devices and people are all connected together: the Internet of Everything (IoE). Although network communication makes life more convenient, it also exposes users to cybersecurity risks, such as malware, phishing, etc. Therefore, it is of utmost importance to conduct cybersecurity education not only for the people who work/will work in IT or security-related professions, as discussed so far, but also for ordinary people, who represent the vast majority of Internet users.

Cybersecurity literacy education (also known as "cybersecurity awareness training") is currently conducted mainly through e-learning programs. However, for non-technical content too hands-on experience is essential. For instance, we believe that the practical ability to recognize phishing emails and websites is more important than the abstract knowledge of what phishing emails and websites are, which is the knowledge typically tested in e-learning courses. Such practical skills can only be acquired through actual exposure to cybersecurity issues, which can only be experienced safely in a controlled education and training environment.

We are currently investigating how hands-on training environments can be used for cybersecurity literacy and similar non-technical education programs. We envisage that gamification could play an important role in this context for increasing the trainees' motivation and information retention rate. This is very important since the target of awareness training programs are often people with little or no interest in low-level computer issues. Moreover, such training will also need to address young Internet users, potentially even starting in primary school, who have limited knowledge about computing and networking.

In this context we are planning to explore the concepts put forward by [15], as we aim to develop a learning platform that shapes the security content in a storytelling manner, so as to engage the trainees emotionally, thus improving the effectiveness of the training. We believe that content personalization and training automation would also play important roles in providing an engaging learning experience.

5 Conclusions

In this paper we have presented the major cybersecurity education and training programs in Japan, and used them as a case study for an analysis of the best practices and methodologies in cybersecurity training. We have systematically analyzed these methodologies through a taxonomy based on training content, activities, and features such as target participants and their expected ability levels. The program comparison from this perspective leads us to conclude that various training programs have become available since 2013, targeting all potential participants and levels of expertise. We expect this will lead to a significant increase in the skill level of IT and security professionals in Japan.

The methodology analysis also served as foundation for defining requirements that must be met in order to ensure the effectiveness of cybersecurity education and training. In this context we have introduced the activities of the Cyber Range Organization and Design chair at JAIST towards furthering

cybersecurity education and training. A main contribution in this context is the design and implementation of a training support framework that satisfies the said requirements.

6 Acknowledgments

The authors would like to thank the organizers of the CYDER and Hardening Project programs for providing us with the opportunity to attend several training sessions of these programs, either as observers or as participants. The first-hand experience with these training activities proved invaluable in developing our training analysis methodology.

References

[1] DEF CON Hacker Convention. https://www.defcon.org/.

[2] Moodle – Open-source learning platform. https://moodle.org/.

[3] Jonathan Burket, Peter Chapman, Tim Becker, Christopher Ganas, and David Brumley. Automatic Problem Generation for Capture-the-Flag Competitions. In *Proceeding of the 2015 USENIX Summit on Gaming, Games and Gamification in Security Education (3GSE'15)*, 2015.

[4] enPiT University Consortium. enPiT-Security (SecCap) Training Program (in Japanese). https://www.seccap.jp/.

[5] Japan Network Security Association (JNSA). Security Contest (SECCON) (in Japanese). http://seccon.jp/.

[6] Ministry of Internal Affairs and Communications, Japan. Cyber Defense Exercise with Recurrence (CYDER) Training Program (press release). http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130925_02.html.

[7] National Center of Incident Readiness and Strategy for Cybersecurity, Japan. http://www.nisc.go.jp/eng/index.html.

[8] National Center of Incident Readiness and Strategy for Cybersecurity, Japan. Cybersecurity Strategy (in Japanese), 2013.

[9] National Institute of Information and Communications Technology, Japan. Hokuriku StarBED Technology Center. http://starbed.nict.go.jp/en/index.html.

[10] Nomura Research Institute – Secure Technologies. Secure Eggs Training Program (in Japanese). http://www.nri-secure.co.jp/service/learning/secureeggs.html.

[11] Nomura Research Institute (NRI) SecureTechnologies. http://www.nri-secure.com/.

[12] C. Pham, D. Tang, K. Chinen, and R. Beuran. CyRIS: A Cyber Range Instantiation System for Facilitating Security Training. In *Proceedings of the International Symposium on Information and Communication Technology (SoICT)*, 2016.

[13] SANS Institute. SANS NetWars Training Courses. https://www.sans.org/netwars.

[14] Karen Scarfone, Murugiah Souppaya, Amanda Cody, and Angela Orebaugh. National Institute of Standards and Technology – Technical Guide to Information Security Testing and Assessment, 2008.

[15] Lee Sheldon. Game-Based Learning, Collateral Learning, and Beyond. In *Proceedings of the 2015 USENIX Summit on Gaming, Games and Gamification in Security Education*, 2015.

[16] Web Application Security Forum. Hardening Project (in Japanese). http://wasforum.jp/hardening-project/.