DOI 10.15302/J-SSCAE-2016.06.009

Certification for Cyberspace Security Professionals in China

Zhang Hongli[1], Yu Haining[1], Fang Binxing[2], Qin Yuhai[3], Yu Xiangzhan[1], Chu Chengyuan[2]

1. School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China
2. Cyber Security Association of China, Beijing 100010, China
3. National Police University of China, Shenyang 110854, China

Abstract: Professional certification and vocational training are important aspects of cyberspace security talent cultivation, as they allow talent to grow rapidly while continuously improving the technical level and practical ability of existing employees. First, this paper surveys the current conditions of professional certification and vocational training. The authors then analyze the main problems of cyberspace security professional certification and vocational training. Finally, the authors propose a system of professional certification and vocational training.

Keywords: cyberspace security; workforce framework; professional certification; vocational training

1 Introduction

Cyberspace security professional certification evaluates whether practitioners have mastered the relevant technical knowledge and developed the skills and abilities to work independently. Establishing cyberspace security professional certification systems facilitates talent cultivation by promoting the quality and professional level of practitioners, unifying professional standards, promoting the process of the global standardization of local certification, and ensuring that the cyberspace security certification is internationally recognized and respected. Compared with traditional academic education, vocational training in cyberspace security is relevant, flexible, and practical. These benefits warrant establishing vocational training systems that can rapidly expand the cyberspace security talent team while also continuously improving the technological level and practical ability of existing talent. Establishing a system for professional certification and vocational training plays an important role in cyberspace security talent cultivation.

2 Cultivating cyberspace security talent both at home and abroad

Compared to China, the United States and other developed countries place a greater emphasis on vocational training and professional certification for cyberspace security. Responding to developments in the cyberspace security situation, these countries propose strategic planning at the national level to improve their training and certification systems. The National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence (CAE) in information assurance and cyber defense (IA/CD) programs. The goal of these programs is to reduce vulnerabilities in the United States' national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines [1]. By September 2016, the NSA and DHS had approved 209 institutions as CAE Designated Institutions [2]. The CAE model can be abstractly divided into four steps: the

Received date: 12 October 2016; **revised date:** 20 October 2016

Corresponding author: Zhang Hongli, School of Computer Science and Technology, Harbin Institute of Technology, Vice Dean and Professor. Major research field is network and information security. E-mail: zhanghongli@hit.edu.cn

Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)

Chinese version: Strategic Study of CAE 2016, 18 (6): 044–048

Cited item: Zhang Hongli et al. Certification for Cyberspace Security Professionals in China. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.009

uniform definition of knowledge units and key areas, the uniform formulation of CAE standards, the mapping of applicants' educational and training resources onto required knowledge units, and a uniform review of the degree of match of the mapping.

In 2012, the United States officially released the National Initiative for Cybersecurity Education (NICE) Strategic Plan [3], clearly indicating their interest in training and developing cyberspace security talent, in order to build and maintain a competitive and professional team that has the best cyberspace security talent. The United States released the latest version of the NICE Cybersecurity Workforce Framework in 2014, and this framework is continually adjusted and updated. In 2013, the European Commission issued the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, which stated that cybersecurity and information security training should start from the national level. In 2013, Japan issued the Cybersecurity Strategy, which clearly pointed out that the personnel training of cybersecurity and information security should be an important measure in establishing a cyberspace security certification and training system.

Overall, the main measures taken by developed countries to establish their professional certification and vocational training systems include: ① at the national level, making a cyberspace security strategy plan that emphasizes the important position of professional certification and vocational training; ② the state distributing the authority to coordinate, implement, supervise, and manage the system to different government departments that will jointly participate in and promote the building of training and certification systems and implement the relevant policies and legislation of cyberspace security training and certification; ③ eormulating a cyberspace security workforce framework and defining uniform general terms to describe the professional categories, vocation paths, post abilities, and qualifications.

The international construction of the cyberspace security professional certification and vocational training systems framework started early. Advanced cyberspace security training and certification systems have already been established, and scalable training and certification industries have been formed. The framework includes: ① the government that formulates policies for carrying out the relevant training and certification; ② industry associations that help to set cyberspace security professional certification and vocational training standards, establish and update practical certification projects, carry out continuous professional training activities, organize certification examinations, and award certificates; ③ universities and research institutes that assist in the development of training and certification systems and that carry out education and training activities; and ④ enterprises and manufacturers that carry out internal non-certified vocational training for employees and issue the corresponding training certificates. At present, cyberspace security certification and training systems established by certain associations have higher authority and recognition, such as the International Information System Security Certification Consortium (ISC) [2,4], Information Systems Audit and Control Association (ISACA) [5], International Council of E-Commerce Consultants (EC-Council) [6], and Computing Technology Industry Association (CompTIA) [7].

China urgently needs cyberspace security talent; the number of talented professionals is low, and with the development of informatization construction, the demand for cyberspace security talent will continue to increase every year. By 2020, the estimated demand for cyberspace security talent will exceed 1.4 million. According to the survey of information security vocational training at colleges and universities, a document from the General Office of the Ministry of Education of the People's Republic of China (No. 4 [2014]), the average annual employment rate of information security postgraduates is no less than 97% and the average annual employment rate of undergraduates is no less than 95%; both these percentages are far higher than for other professions.

At present, although China has tried to develop professional education in cyberspace security, the demand for such talent is difficult to satisfy. The Ministry of Education first established a college major in cyberspace security in 2002; between 2002 and 2013, the Ministry of Education approved a total of 96 colleges nationwide to establish information-security-related majors through regular college courses, which include information security (85), information countermeasures (17), and security management (12). These colleges produce approximately 10 000 graduates each year, but their aggregate number has not yet surpassed 80 000. In June 2015, the Office of the State Council Academic Degrees Committee established cyberspace security as a first-class discipline [8] and approved 29 colleges to offer doctoral degrees [9]. The establishment of cyberspace security as a first-class discipline laid a solid foundation for training cyberspace security talent. However, considering the annual talent gap of 500 000 professionals each year, solving the problem of large-scale cybersecurity vocational training remains challenging in the short term. Therefore, professional certification and vocational training of on-post staff should be developed immediately to increase their technical levels and practical skills.

3 Problems in cyberspace security professional certification and vocational training

Over the years, China has developed a cyberspace security professional certification and vocational training system, such as the Certified Information Security Professional (CISP) certification and related authorization training. However, China's current cyberspace security training system is imperfect because it is difficult to meet the strategic demand of "strengthening the building of cyberspace security talent." Its main problems include:

3.1 The lack of a cyberspace security workforce framework hinders the development of professional certification and vocational training

China has not yet established a uniform definition of cyberspace security work and professional talent; departments differ significantly in vocations, job responsibilities, and other related aspects. The lack of a common language to discuss and understand the work and skills requirements of cybersecurity professionals has created significant obstacles to creating security skills baselines, identifying skills gaps, establishing relevant positions, and conducting professional certification and vocational training.

3.2 The professional certification and vocational training system construction is lagging, the acceptance of certification needs to be improved, and the training market needs to be standardized

An accreditation system can help certifying organizations to establish internal management and professional certification systems, improve the level of management, and maintain good performance. The lack of an accreditation system has seriously affected the authority of certification practices, so that it is difficult to secure the recognition of practitioners and employers. China lacks an authorized system of cyberspace security professional training institutions, and particularly the regulation of domestic training institutions providing international certified training services. The lack of oversight of vocational training institutions allows the dissemination of false advertising and illegal operations, seriously affects the vocational training market order, and impairs the reputation of cyberspace security vocational training.

3.3 The knowledge systems of cyberspace security professional certification and vocational training need to be improved

Cyberspace security is a challenging new field that requires a wide breadth of knowledge from multiple fields and a short update cycle. China should develop and update certification and training based on these features. Currently, there are few certification programs in China. Further, these programs are out of touch with necessary knowledge, require a long time to be updated, and have not yet formed a hierarchical and complementary knowledge system. These characteristics are not consistent with knowledge in the domain of cyberspace security, and therefore do not promote position skills and promotion.

3.4 There are few professional training institutions and the training scale is limited

There are few professional training institutions in China, and training at many institutions is limited to cyberspace security products, consulting, or business evaluation rather than certification, which means there are few trained staff in China. In addition, the lack of professional training institutions also provides an opening to other institutions that lack training capabilities to fish in troubled waters.

3.5 Cyberspace security professional training institutions vary in ability, and training quality needs to be improved, especially the quality of practical skills training

China's professional training institutions differ in their faculties, curriculum, experimental environments, and other aspects, and the quality of training needs to be improved in all these aspects. With regards to faculty, China lacks an accreditation system for instructors; as a result, there are few instructors and their abilities vary. As for the curriculum, most instructors use short-term training to summarize the examination outline and analysis questions, and this training lacks durable and systematic curricula. Turning to the experimental environment, most remain at the stage of teaching theoretical knowledge without bridging the gap between theory and practice, which leaves students lacking the skills and practical abilities they need for a real job. This is unfortunate considering that famous international institutions support increasingly elaborate and effective experimental environments. For example, the EC-Council's iLabs experimental platform covers 270 kinds of common hacker attack techniques, supports the construction of more than 140 models of real-time scenarios, and provides more than 2 200 kinds of common hacker tools. The ECSA and LPT certification established the by EC-Council can examine the applicant's practical skills on the iLabs platform.

4 Policy suggestions

To accelerate the construction of a system of cyberspace security professional certification and vocational training in China, the authors propose that the Cyber Security Association of China (CSAC) should establish a cyberspace security professional certification and vocational training system for China that will directly provide certification services, authorize training activities, quickly enlarge the talent pool, and continually improve existing employees' technical levels and practical abilities. Specific measures include: ① reforming training and certification institutions, standardizing management systems, and developing measures for promotion; ② vigorously promoting the construction of a cyberspace security workforce framework, establishing a national unified system of cyberspace security posts and standards for the employees' knowledge, skills, and abilities, and constructing a certification knowledge system to define all certification knowledge areas, associate blocks of knowledge with corresponding jobs, improve the match between certification and jobs, and strengthen the popularity and acceptability of certification; ③ vigorously supporting the development of cyberspace security vocational training, speeding up infrastructure construction, implementing instructor training to regulate the training markets, expand the scale of training, and improve training quality; ④ establishing certification institutions, training institutions, and university resource-sharing systems, breaking down boundaries, gathering resources, and realizing the cross-border rotation of talents.

4.1 Reforming training and certification institutions, standardizing management systems, and developing measures for promotion

The CSAC should directly provide cyberspace security professional certification services, organize certifying examinations, issue certifications, and authorize cyberspace security vocational training. In addition, the CSAC should establish a post-holder certification system for cyberspace security work, an accreditation authorization system for training institutions, certification standards for training instructors, and post-holder certification of training instructors. Moreover, the relevant measures for promotions should be formulated to ensure that all the institutions are workable. By having the association directly support the certification service, the unified cyberspace security professional certification institution will benefit from increased authority and fairness, which will facilitate the employment of certified personnel. Authorizing training activities by the association will enable standardization of the market order and enlargement of scale, and will promote the quality of vocational training.

4.2 Vigorously promoting the construction of a cyberspace security workforce framework and establishing a certified knowledge system

The CSAC should formulate the "cyberspace security workforce framework" to reflect the current status of China's cyberspace security. It defines the work and general vocabulary for China's cyberspace security, and it also describes the standards of responsibilities for each job, including the knowledge, technologies, and abilities that are needed by staff. It is based on the workforce framework to build the knowledge certification system and define the knowledge fields of various kinds of certification, the blocks of knowledge, and the corresponding jobs. It traces the leading edge of domestic cyberspace security technology at regular intervals to ensure the system continually upgrades and updates.

4.3 Establishing and updating the cyberspace security professional certification project system

Facing demands from all kinds of enterprises, the CSAC has organized colleges, research institutes, and security enterprises to establish the certification project system. This system, which is based on the cyberspace security workforce framework, has several different types of clearly classified certifications that complement each other. This system covers all certification projects and publishes their knowledge areas, exam outlines, and relevant textbooks.

4.4 Vigorously supporting the development of cyberspace security vocational training, speeding up infrastructure construction, and implementing instructor training project

China should introduce preferential policies in finance, business, taxation, and consulting to support the establishment and development of cyberspace security training institutions, gradually form a vocational training network covering the whole country, and make vocational training available to everyone at any time or place. For innovative training institutions, the government should deploy real-time simulation platforms and award those training institutions that have enhanced training quality to help promote advanced training experience and results. The CSAC should implement an instructor training project, formulate a training system, establish classes, and conduct training.

4.5 Establishing a resource-sharing system for certification institutions, training institutions, and universities

Colleges and universities bring together a large number of cyberspace security resources; a resource-sharing system for certification institutions, training institutions, and colleges and universities should be established in these institutions, especially regarding the sharing of teacher resources. Colleges and universities should be encouraged to carry out vocational training for cyberspace security, establish mutual authentication systems between training instructors and university teachers, and inject high-quality and stable teacher resources into the cyberspace vocational training market.

5 Conclusions

Professional certification and vocational training are important parts of China's cyberspace security talent development, constituting the two main forms of cyberspace security talent cultivation alongside academic education. It is necessary to recognize the current problems in China's training and certification system so that all stakeholders can cooperate to establish and develop a certification and training system, improve talent team training, and support the development of cyber power.

References

[1] White House. The comprehensive national cybersecurity initiative [EB/OL]. [2016-09-10]. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[2] National Security Agency. NSA/DHS CAE institutions [EB/OL]. [2016-10-10]. https://www.iad.gov/nietp/reports/current_cae_designated_institutions.cfm

[3] National Initiative for Cybersecurity Education. NICE [EB/OL]. [2016-09-10]. http://csrc.nist.gov/nice/.

[4] International Information System Security Certification Consortium. (ISC)^2 [EB/OL]. [2016-09-10]. https://www.isc2.org/.

[5] Information Systems Audit and Control Association. ISACA [EB/OL]. [2016-09-10]. https://www.isaca.org/Pages/default.aspx.

[6] EC-Council. EC-Council [EB/OL]. [2016-09-10]. https://www.eccouncil.org/.

[7] Computing Technology Industry Association. CompTIA [EB/OL]. [2016-09-10]. http://www.comptia.org/.

[8] Ministry of Education of the People's Republic of China. Academic Degree Commission of the State Counter, the Ministry of Education. Notice concerning establishing cyberspace security as a first level discipline ([2015]11) [EB/OL]. (2015-06-11) [2016-09-10]. http://www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_ 221423.html. Chinese.

[9] Ministry of Education of the People's Republic of China. Notice concerning developing cyberspace security first level discipline doctorate authorization ([2015]39) [EB/OL]. (2015-10-30) [2016-09-10]. http://www.moe.gov.cn/jyb_xxgk/moe_1777/moe_1778/201511/t20151127_221424.html. Chinese.