Translation

The following study, by a PRC government cybersecurity center, analyzes the structure of China's complement of cybersecurity and IT security professionals. The study finds that PRC cybersecurity practitioners are still too few in number and are often burdened with non-security-related IT tasks, although China is making progress solving these problems. The authors recommend that all Party leaders take courses on cybersecurity to raise awareness of the importance of the topic.

Title
Research Report on the Status of China's Information Security Professionals (2018-2019)
中国信息安全从业人员现状调研报告（2018-2019 年度）

Author
The China Information Technology Security Evaluation Center (中国信息安全测评中心), a state agency that provides cybersecurity services to the PRC government and large Chinese corporations, is the managing unit (主办单位) for this report. The units contracted (承办单位) to contribute to this report are the Information Security Industry Branch (信息安全产业分会) of the China Information Industry Trade Association (中国信息产业商会); and the GuangDong Information Technology Security Evaluation Center (广东省信息安全测评中心), also known as the China Information Technology Security Evaluation Center (GuangDong Office) (中国信息安全测评中心广东测评中心).

Source
China Information Technology Security Evaluation Center website, September 6, 2019.

The Chinese source text is available online at:
https://web.archive.org/web/20201007121055/http%3A%2F%2Fwww.itsec.gov.cn%2Fzxxw%2F201909%2FP020190906557330247920.pdf
US $1 ≈ 7 Chinese Yuan Renminbi (RMB), as of December 14, 2020.

Translation Date	Translator	Editor
December 14, 2020	Etcetera Language Group, Inc.	Ben Murphy, CSET Translation Lead

◆ Index of Figures

1. Overview

Cyberspace competition is, in the final analysis, a talent competition. As the new science and technology (S&T) revolution continues and industries upgrade, information technology is fundamentally changing the way people live and shaping new patterns of economic and social development and national security. Information security talent will play a critical role in this process of transformative development. Given the challenges and opportunities of this new era, the question of whether it is possible to effectively promote the development of information security talent will become an issue of paramount importance in implementing the cyber powerhouse[1] strategy. It will also be critical to gaining the initiative in a setting of increasing international competition.

Since the 18th Party Congress [in 2012], the state has taken a series of important actions concerning the development of cybersecurity talent. It has introduced several powerful measures which have achieved successes that are obvious to all. Breakthrough progress has been made in establishing cybersecurity curricula, specializations, academic departments, and degree-granting programs. Cybersecurity has progressed rapidly in the areas of on-the-job training and professional certification testing. Cybersecurity attack-and-defense training exercises and skill competitions have seen vigorous growth. Cybersecurity talent and innovation bases have been planned and built in multiple locations, and have introduced policies for talent cultivation and recruitment. Important industries are strictly implementing cybersecurity responsibility systems and personnel compliance requirements while accelerating implementation of security personnel training and management regimes. The departments concerned launched in-depth propaganda and education efforts, significantly heightening cybersecurity consciousness throughout society.

China is currently presented with a major strategic opportunity to develop information security talent. In-depth research is necessary now and for a while into the future to track the current status of information security practitioner teams, to explore the growth patterns of information security talent, and to analyze problems present at the deeper levels of the effort to build talent teams. This “Research Report on the Status of China's Information Security Professionals (2018-2019)” is a major investigative activity sponsored by the China Information Technology Security Evaluation Center and contracted out to the Information Security Industry Branch of the China Information Industry Trade Association. This report, which employed such approaches as online questionnaire surveys, front-line on-site interviews, and consultations and discussions with experts, entailed an in-depth investigation according to six major dimensions into the current status of information security professionals and the current talent environment in the expectation of providing practical guidance for security industry talent work innovation development and of providing a decision-making reference for building cyber and information security talent teams in China.

I. Main Study Results

[1] Translator's note: The Chinese word 强国, literally "strong nation," is translated as "powerhouse" throughout this translation. An acceptable alternate translation for the term 网络强国—rendered here as "cyber powerhouse"—is "cyber superpower." For a detailed discussion of this term, see: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/lexicon-wangluo-qiangguo/

II. Existing Issues

III. Suggested Solutions

IV. Study Methods

I. Main Study Results

This study consists of an in-depth analysis of the current status of information security professionals and the current talent environment according to the six dimensions of study subjects, work conditions, mobility and allocation, ability enhancement, institutional environment, and security situation. All matters of concern, including the differentiation of practitioner populations, education and training, assessment and evaluation, motivation assurance, team building, and implementation of talent-related policies and regulations received comprehensive coverage.

(I) Study Subjects

The report included the first definitions and classifications of professionals in this nontraditional field of information security. The study subjects were clearly defined as “personnel whose social division of labor and source of income are primarily based on information security work duties.” Moreover, the work roles of information security professionals were divided into six major categories and 14 subcategories. The study showed that the largest numbers of information security professionals were found in security operations (62.4%) and security development (32.4%). 45.5% of professionals were employed by private enterprises, 19.3% by state-owned enterprises (SOEs), and 16.5% by government agencies and public institutions. Nearly forty percent (38.4%) of professionals had participated in combat-type cybersecurity contests.

(II) Work Conditions

An important indicator of whether the security work at a unit is fully in place is whether or not it has established a professional information security team of an adequate size. The study data shows that, with the exception of information security professional service enterprises, especially large enterprise groups, and large internet enterprises, all of which establish relatively large-scale information security talent teams, 50% of government and business units had information security teams with fewer than 20 members. Nearly sixty percent of information security professionals were required to take on non-information security work responsibilities. The “one person with multiple jobs” phenomenon was most striking among information security staff at government agencies and public institutions.[2] There are shortages of various types of talent, especially talent who do security development and planning and management work.

(III) Mobility and Allocation

The average annual salary among information security professionals was 153,000 yuan Renminbi (RMB), which continued a trend of year-on-year compensation increases, but the magnitude of the increase declined. 42.9% of information security professionals experienced obvious work stress, but the majority were optimistic about their career development prospects. The rate of talent mobility slowed in the past three years. The factors which affected occupational

[2] Translator's note: "Public institutions" (事业单位) are organizations created and led by PRC government departments that provide social services. Unlike state-owned enterprises (SOEs), public institutions do not create material products and do not generate income. Public institutions are not considered government agencies, and their employees are not civil servants. Most public institutions are fully or partially government-funded, but some fully privately funded (but still government-led) public institutions exist. Public institutions typically provide services in areas such as education, science and technology, culture, health, and sanitation.

mobility were, in order of importance: “compensation,” “opportunity for career advancement,” “work atmosphere,” and “self-realization of values.” This indicates that practitioners attach considerable importance to the benefit and development factors of work.

(IV) Ability Enhancement

In this study, “occupational training” replaced the previous year’s “self-taught learning” as the ability enhancement method that information security professionals were most likely to choose (68.8%). There was a demand among practitioners for ability enhancement in various narrowly defined orientations. The greatest demand was for big data security, followed in order by cloud security, security management, and penetration testing. Among the various types of information security certificates, the Certified Information Security Professional (CISP) credential was both the most commonly held (71.8%) and the most sought after (68.9%) by practitioners.

(V) Institutional Environment

Specialized personnel in specialized positions engaging in specialized work is an embodiment of professionalization. Nearly seventy percent of the units where information security professionals were employed had set up specialized cybersecurity management departments and officers, but 57.7% of these personnel were concurrently responsible for other non-security work; the “personnel-post mismatch” phenomenon was quite widespread. 65.5% of the units where practitioners were employed had set up career advancement channels and work incentive mechanisms, but fewer than two-tenths felt that the mechanisms in question were “implemented effectively.” 43.7% of practitioners believed that they their job titles could not be clearly categorized, which was an obvious increase over the previous year (25.9%). 63% of practitioners needed to undergo some form background check prior to employment.

(VI) Security Situation

The information security threats which practitioners most often faced were vulnerability attacks, data leaks, and denial-of-service (DoS) attacks, in that order. The main reasons that information security events occurred were imperfect management, lack of security training, management neglect, and insufficient talent and resources. 78.0% of units where practitioners were employed had established internal cybersecurity policies and operating procedures, but only one-fourth report that they had been effective. 77.6% of practitioner-employing units had launched information security risk evaluation efforts. “Chips” replaced the previous year’s “operating systems” as the core technology considered by respondents to be the one China most needs to achieve domestic production of (国产化).

II. Existing Issues

There remains a rather large gap between the current skill structure of information security talent teams and the needs of economic and social development and national security. This study shows that China’s effort to build information security talent teams still suffers from the following outstanding problems.

(I) All-Around Shortage of Information Security Professionals

Whether it relates to a work layer such as data, applications, systems, or networks or to a business process such as R&D, system building, operations, management, or production, each link in the effort to informatize the entirety of information security work requires someone to assume information security work duties. However, there currently exists a state of overall shortage of information security professionals in China. This shortage is manifested in the following: 1) The total number of information security personnel is insufficient; 2) a large amount of information security work is completed on a "part-time" basis; 3) there are shortfalls in each type of security work role.

(II) Professionalization of Information Security Is Still in the Initial Stages

Information security professionalization consists of the standardization of the professional knowledge, skills, and rules of conduct for information security professionals. An embodiment of professionalization is specialized personnel in specialized positions engaging in specialized work. Nearly seventy percent of the units where information security professionals are employed have already set up specialized cybersecurity management departments and officers. However, the professionalization of information security is, overall, still in the initial stages of development. First, information security still lacks a unified professional (group) standard. Second, the "personnel-post mismatch" is widespread in information security. Third, social awareness of information security occupations is weak, especially in employer senior management.

(III) The Difficulty in Meeting the Demand for Personnel Ability Enhancement

The ability of employers to provide sufficient training, continuously improve the professional skills of talent, and help them to achieve self-realization of values will play an increasingly important role in "talent attraction" and "talent retention." At present, the universal difficulty in meeting the demand for personnel ability enhancement is manifested in the following: 1) The thriving demand for enhancement of practitioner abilities; 2) practitioners' expectations of obtaining professional credentials; 3) insufficient investment by employers in education and training.

(IV) Impediments in Institutional Mechanisms for Information Security Talent

Cyber and information security is an interdisciplinary, non-traditional industry that crosses boundaries and merges with other industries. Thus, only institutional mechanisms that encourage innovative development can allow the creativity of talented people to compete and blossom and their ability and intelligence to gush forth. There still exist a series of institutional impediments to the development of information security talent: First, the methods for assessing security practitioners are insufficient; second, personnel incentive mechanisms are unsound; third, mechanisms for guiding talent to important and critical fields are lacking.

III. Suggested Solutions

The implementation of cyber powerhouse strategy deployments in the new era requires that we take Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, in particular his thinking on cyber powerhouse strategy, as a guide. We should place talent-related work in an even more prominent strategic position, further raise the importance and urgency of information security talent work, make use of our great power (大国) advantages and institutional advantages, and push forward with the effort to raise information security awareness and abilities throughout society and especially to enhance the skills of information security professionals.

(I) Establishing a Systematic Information Security Talent Development Plan

From the high perspective of raising information age productivity, and making the building of globally competitive cybersecurity talent teams our goal, let us carry out systematic, advanced planning and deployments with regard to the overall situation of national cyber and information security talent development: 1) Build a cybersecurity national education and continuing education system; 2) make a unified plan to push forward with overall cybersecurity talent development work; 3) with the collaboration of multiple entities, jointly build a cybersecurity talent ecosystem.

(II) Using Science to Push Forward with Professionalization of Information Security Talent

In view of the severe, all-around shortage of information security professionals, professionalization measures will help to make clear the legitimacy of information security occupations, increase the relevance of information security education and training, bring about a balance in information security talent supply and demand, and make information security occupations more attractive. However, different types of practitioners should not be managed by simply using a one-size-fits-all occupational licensing approach. We recommend that, first, in-depth basic theoretical and cutting-edge practical research be launched with regard to information security talent development; that, second, an information security knowledge system that is both relatively stable and dynamic be established; and that, third, information security professional talent credentialing work be pushed forward at authoritative institutions.

(III) Making an Effort to Improve the Numbers and Abilities of Information Security Professionals

Guided by the needs of economic and social development and of national security, let us strengthen the farsightedness and relevance of the work of building a talent cultivation system, establish a lifelong education system that is involved throughout the work of information security practitioner learning, and improve the numbers and overall abilities of information security talent teams through the following: 1) Increasing education and training inputs and work intensity; 2) taking differentiated measures to build information security talent teams; 3) pushing forward with information security education and training supply-side reforms in light of the characteristics of specific fields.

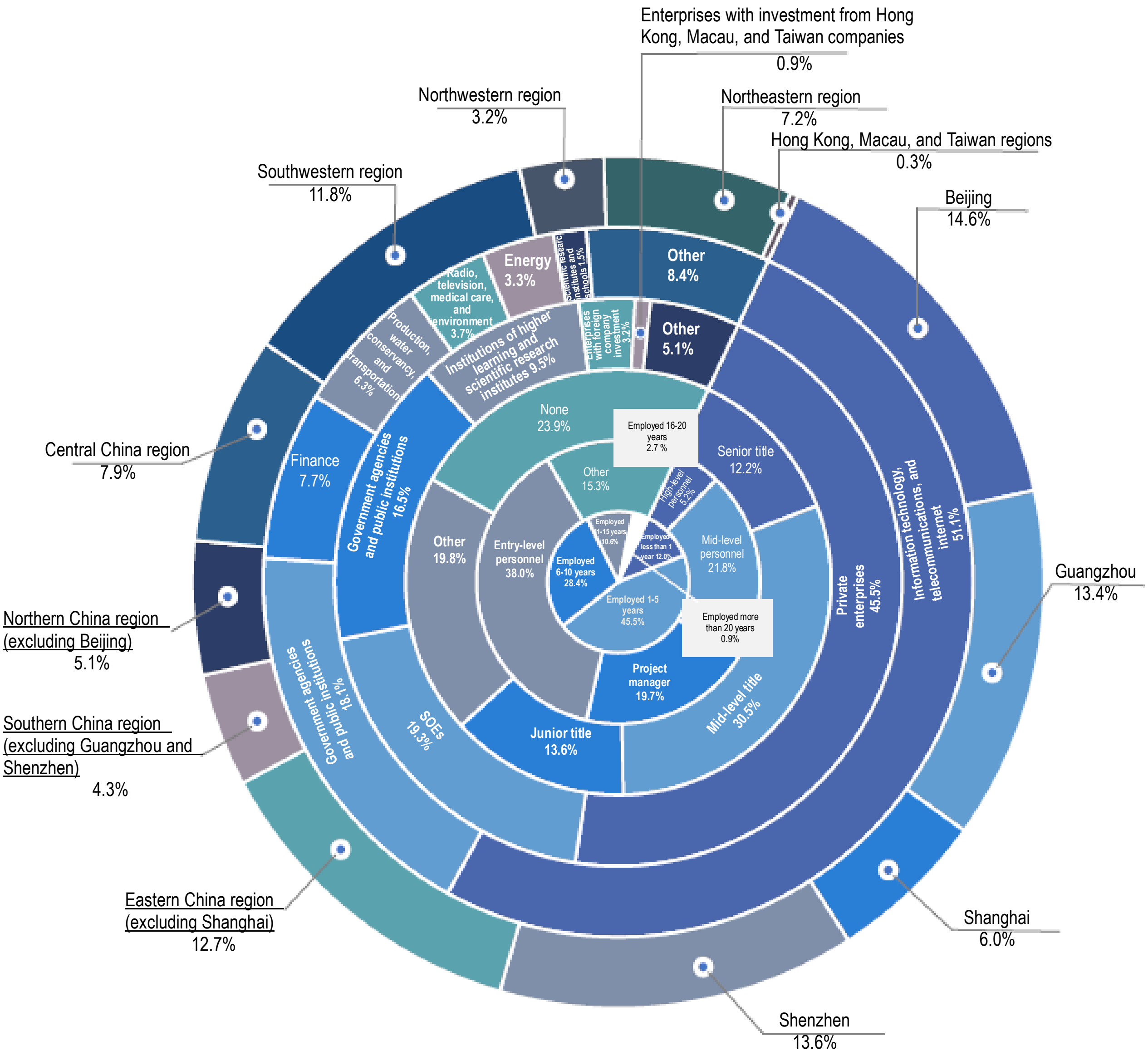
(IV) Continuously Optimizing the Overall Environment for Information Security Talent

Cybersecurity is a cutting-edge field of information technology. It is the field with the greatest concentration of intellectual power and the greatest need for innovation vitality. Let us make utility our watchword (以用为本), give priority to urgent needs, and accelerate innovations in institutional mechanisms for developing information security talent: 1) Raise the cybersecurity consciousness and cybersecurity talent consciousness of leading Party and government cadres at all levels; 2) accelerate innovation of evaluation and incentive mechanisms for information security professionals; 3) establish information security talent guidance and priority assurance mechanisms for key fields.

IV. Study Methods

The 2018-2019 study employed such approaches as an online questionnaire survey, front-line on-site interviews, and consultations and discussions with experts to conduct an in-depth investigation into the current status of information security professionals. The online questionnaire survey collected 4,349 valid samples covering all Chinese provinces, cities, autonomous regions, and directly administered municipalities and encompassing all important industries and fields of critical infrastructure. With regard to the study's dimensions and content, the report considered six major dimensions reflecting the basic situation of information security professionals. It included a comprehensive analysis of their career development, ability enhancement, and mobility and allocation.[3]

[3] [Translation of footnote in the Chinese source text] In keeping with the current actual practice of the industry, this report treats the phrase "information security" (信息安全) the same as "cyberspace security" (网络空间安全) and "cybersecurity" (网络安全) broadly defined and does not strictly differentiate between them according to their academic meanings.



2. Study Subjects

Ever since information security work appeared, the issue of how to define practitioners and their work duties has received serious attention and has been under continual discussion. Information security is cross-disciplinary and intersects and merges with other fields. As a result, the categories of information security work are extremely diverse. Uniform occupational standards and ability requirements have yet to take shape. The study found that the use of differently defined standards and statistical specifications could have a major effect on a unit's information security team size, i.e., the size of the unit could be several times large or smaller. To facilitate the study and promote the R&D of information security talent standards in China, the study defined and categorized information security professionals for the first time and used these definitions and categories as a sampling basis for defining study subjects.

The report defines information security professionals as “personnel whose social division of labor and source of income are primarily based on information security work duties.” We divided information security professional work roles into six major categories and 14 subcategories based on differences in work content: 1. Regulatory governance, including strategic laws and regulations and enforcement and supervision; 2. planning and management, including strategic planning and organizational management; 3. security development, including analysis design and development and integration; 4. security operations, including security operations and maintenance, data handling, emergency response, auditing, and evaluation and security situation analysis; 5. content security; 6. scientific research and education, including security research, training, and teaching. One practitioner may be responsible for multiple work roles. The practitioner-work role relationship is one-to-many. In this chapter, the study is presented with regard to four areas: Work roles, years of employment, information on the unit where employed, and competition experience.

I. Work Roles

II. Years of Employment

III. Information on Work Unit Where Employed

IV. Competition Experience

Work Roles

The major work role categories that had the highest numbers of information security professionals were security operations (62.4%) and security development (32.4%). The work role subcategories with the largest concentrations of practitioners were security operations and maintenance (22.2%), organizational management (20.6%), development and integration (17.6%), and auditing and evaluation (17.5%), which is primarily carried out by third parties.

Years of Employment

The majority of information security professionals in China have been employed for fewer than ten years, and the largest proportion (45.5%) had 1-5 years of employment. Those who have had more than 10 years of work experience in one field are generally considered to have higher professional skills and work abilities. The study shows that 14.2% of information security professionals in China have more than 10 years of employment, 2.6 more percentage points than in the previous year.

Information on Work Unit Where Employed

The largest proportion (45.5%) of information security professionals had positions in private enterprises (私营企业). Next were SOEs (19.3%) and government agencies and public institutions (16.5%). The associated industry showing the highest concentration was the technology-dense industry of information technology, telecommunications, and the internet (51.1%). The vast majority of units where practitioners were employed had fewer than 300 employees.

Competition Experience

In recent years, all types of enterprises, public institutions, and critical information infrastructure operators have organized and participated in cybersecurity attack and defense challenges, red team-blue team contests, and skill competitions, and the enthusiasm has been unprecedented. Actual combat exercises have played an important role in selecting, promoting, and training cybersecurity talent. The study shows that nearly forty percent (38.4%) of practitioners stated that they had participated in an actual combat-type cybersecurity competition.

I. Work Roles

This study was the first to differentiate between six major categories of work roles (see Figure 2-1).

1. Regulatory governance	Formulation of strategies and regulations
	Information security enforcement and supervision
2. Planning and management	Strategic planning
	Organizational management
3. Security development	Analysis design
	Development and integration
4. Security operations	Security operations and maintenance
	Data handling
	Emergency response
	Auditing and evaluation
	Security situation analysis
5. Content security	Content security
6. Scientific research and education	Security research
	Training and teaching

Figure 2-1 Categorization chart of six major information security work roles

The greatest number of information security professionals were responsible for the security operations (62.4%) and security development (32.4%) work roles (see Figure 2-2). Security operations includes security operations and maintenance (22.2%), auditing and evaluation (17.5%), emergency response (9.9%), data handling (9.0%) and security situation analysis (3.8%). Security development includes analysis design (14.8%) and development and integration (17.6%). The other work role categories were planning and management (26.9%), scientific research and education (17.2%), regulatory governance (16.7%) and content security (7.8%).

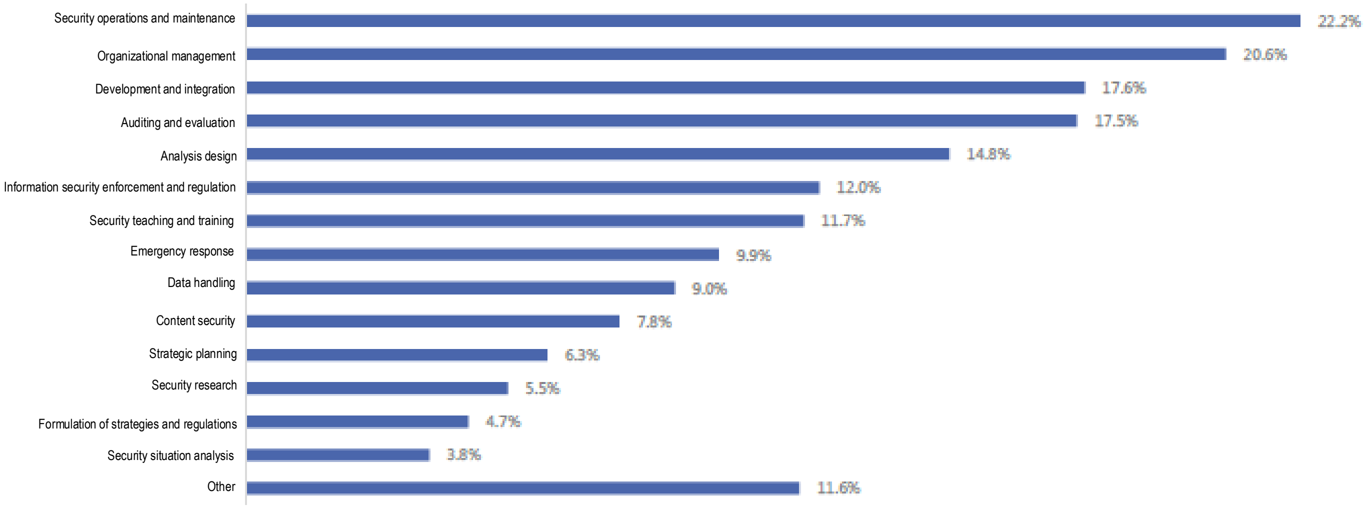


Figure 2-2 Respondent work roles (sample size: 4,349)

II. Years of Employment

The sample data shows that the majority of information security professionals in China now have been employed for fewer than ten years. The largest proportion (45.5%) of these have had 1-5 years of employment. Those with 6-10 years of employment accounted for 28.4%. Information security professionals with more than 10 years of employment accounted for 14.2%, 2.6 more percentage points than in the previous year (see Figure 2-3).

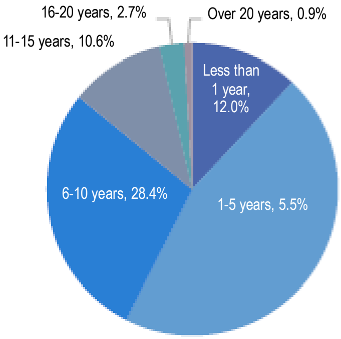


Figure 2-3 Respondent years of employment (sample size: 4,349)

III. Nature of Unit

The sample data of this study shows that the largest proportion (45.5%) of information security professionals had positions in private enterprises (see Figure 2-4). Next were SOEs (19.3%) and government agencies and public institutions (16.5%).

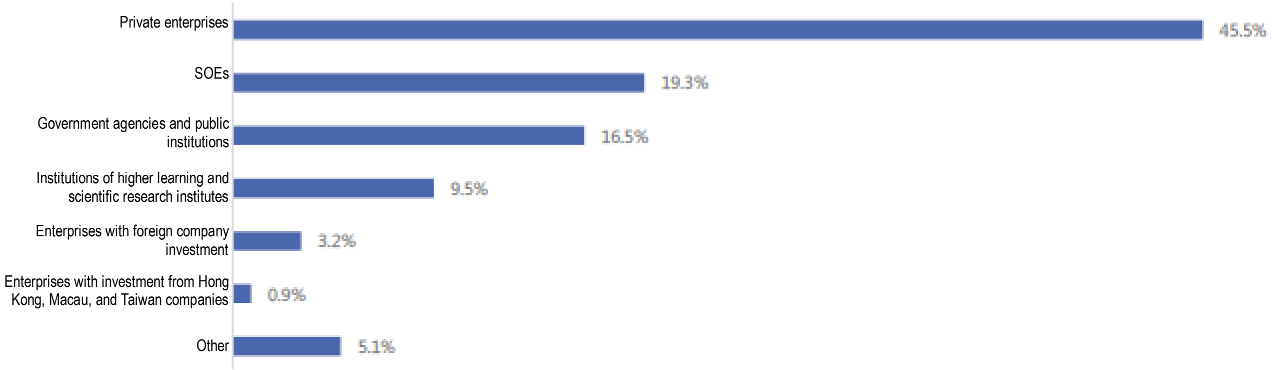


Figure 2-4 Respondent work unit nature (sample size: 4,349)

There was a significant increase in practitioners from SOEs over the previous year. The proportion rose from 8% to 19.3% (see Figure 2-5).

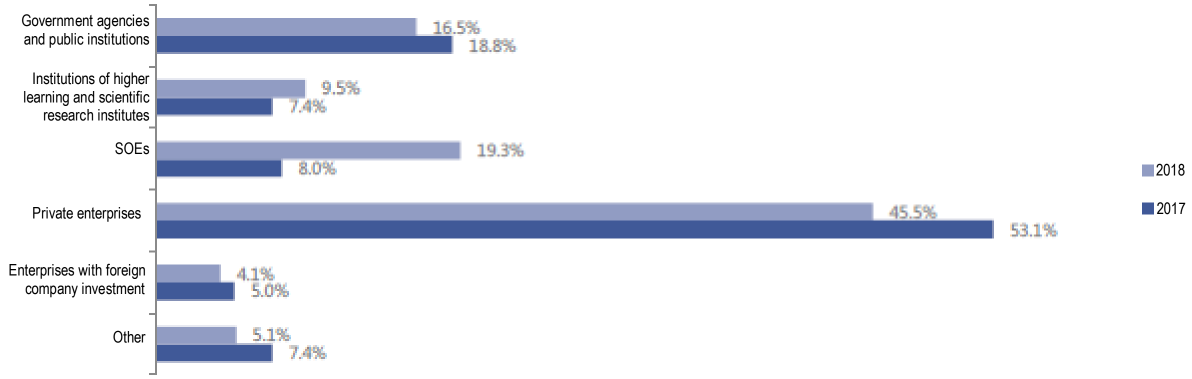


Figure 2-5 Respondent work unit nature, 2017 vs. 2018

IV. Industries

The study data shows that the industry with the highest concentration of information security professionals was the technology-dense industry of information technology, telecommunications, and the internet (51.1%). This was followed by government agencies and public institutions (18.1%), finance (7.7%), and other industries (see Figure 2-6).

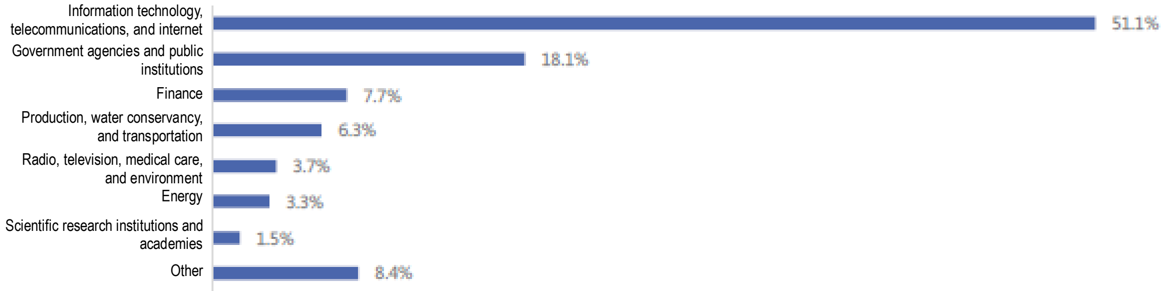


Figure 2-6 Respondent industries (sample size: 4,349)

V. Unit Size

The study shows that the majority of units where information security professionals in China were employed were medium-sized or small enterprises with fewer than 300 employees (55.1%) (see Figure 2-7). The percentage of practitioners at units having more than 1,000 employees was 30.9%. The percentage at units having fewer than 20 employees was the lowest, merely 7%.

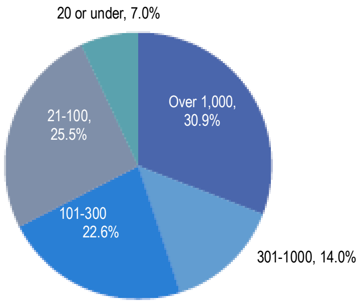


Figure 2-7 Respondent work unit size (number of employees) (sample size: 4,349)

VI. Competition Experience

In recent years, all types of enterprises, public institutions, and critical information infrastructure operators have organized and participated in cybersecurity attack and defense challenges, red team-blue team contests, and skill competitions, and the enthusiasm has been unprecedented. Actual combat (实战) exercises have played an important role in selecting, promoting, and training cybersecurity talent. The study shows that nearly forty percent (38.4%) of professionals stated that they had participated in an actual combat-type cybersecurity competition. The largest proportion (24.1%) participated in online competitions oriented towards professionals in China (see Figure 2-8).

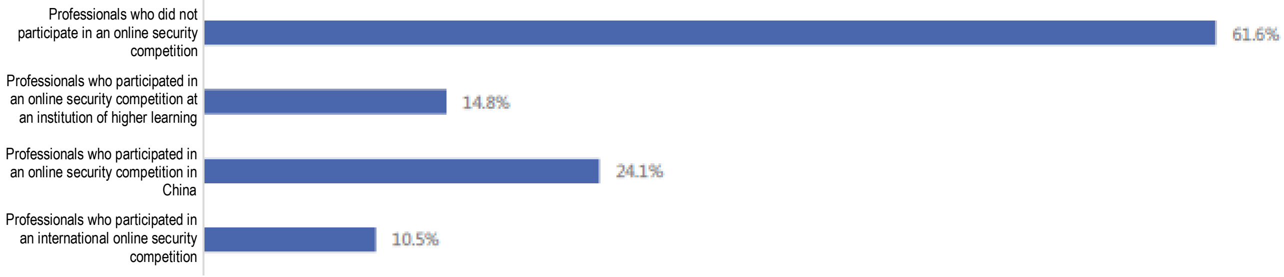


Figure 2-8 Respondent participation in actual combat-type competitions (sample size: 4,349)

3. Work Conditions

The relationship between cybersecurity and informatization (信息化) is like “two wings on one body and two wheels of one engine.” General Secretary Xi Jinping emphasized and pointed out that cybersecurity and informatization complement each other. Security is a precondition for development, and development assures security. Security and development should advance in step with each other. An important indicator of whether the security work at a unit is fully in place is whether or not it has established a professional information security team of an adequate size, and another such indicator is whether or not the security personnel match the overall informatization work.

The study found that information security work is strikingly characterized by a tendency to cross disciplinary boundaries and to intersect and merge with other work. The work duties of practitioners are found in every layer including data, applications, systems, and networks and relate to every business process including R&D, system building, operations, management, and production. In this chapter, the main focus is on investigating the basic situation of information security teams at the units where respondents are employed and the degree and the type of security team personnel shortages. It also introduces two important measures: “Information security personnel as a proportion of informatization staff” and “proportion of information security professionals responsible for non-security work” in order to provide an in-depth picture of how information security talent teams are being built in various organizations.

I. The Situation of Security Teams

II. Personnel Shortages

The Situation of Security Teams

The study shows that, with the exception of information security professional service enterprises, huge enterprises and conglomerates, and large internet enterprises, all of which establish large information security talent teams, 50% of government and business units had information security teams with fewer than 20 members. Personnel who performed information security roles accounted on the average for approximately 36.1% of all informatization staff. The proportion of information security professionals was the highest in the information technology, telecommunications, and internet industry, where the mean proportion was 40.8%. The more people that a unit employs, the larger are the information security teams, and the larger is the proportion of security personnel among informatization personnel. The highest proportion (39.9%) of security teams with more than 500 members was found in units where the total number of people was greater than 1,000. Such units also had the highest percentage (51.2%) of security personnel among informatization personnel.

Personnel Shortages

Nearly sixty percent of information security professionals were required to do work that had no information security content. The phenomenon of requiring “multiple jobs for one person” was most significant in government agencies and public institutions. Among those who were required to additionally perform non-security work, 33.8% of respondents said that non-security work accounted for more than 50% of their everyday work. The majority were of the opinion that the information security personnel teams at their units were of insufficient size to meet current work needs. Entry-level professionals were more likely than intermediate and high-level professionals to feel that there were an insufficient number of information security personnel. Part-time professionals were more likely than full-time professionals to feel that there was an insufficient number of information security personnel. At present, every type of information security work role is suffering from a shortage. From the perspective of security role major categories, we find the most severe shortages in the security development role and the planning and management role. As for subcategories, the roles with the worst shortages are analysis design (35.9%), organizational management (33.5%), and development and integration (30.5%).

I. The Situation of Security Teams

1. Many government and business units have information security teams of 20 or fewer people

Roughly half of information security teams in business and government units in China have no more than 20 members (49.5%). The largest proportion of these is information security teams of 6-20 members, accounting for 28.4%. The proportion of security teams with no more than 5 members is 21.1% (see Figure 3-1).

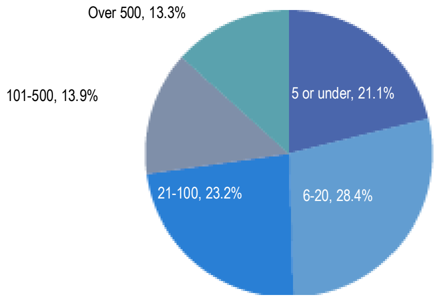


Figure 3-1 Size of information security team at respondent work units (sample size: 4,349)

From the perspective of industry, we find the largest information security teams in government and business units in the information technology, telecommunications, and internet industry, where units with security teams of 100 or more accounted for 41.2%, significantly higher than the mean (27.2%) (see Figure 3-2).

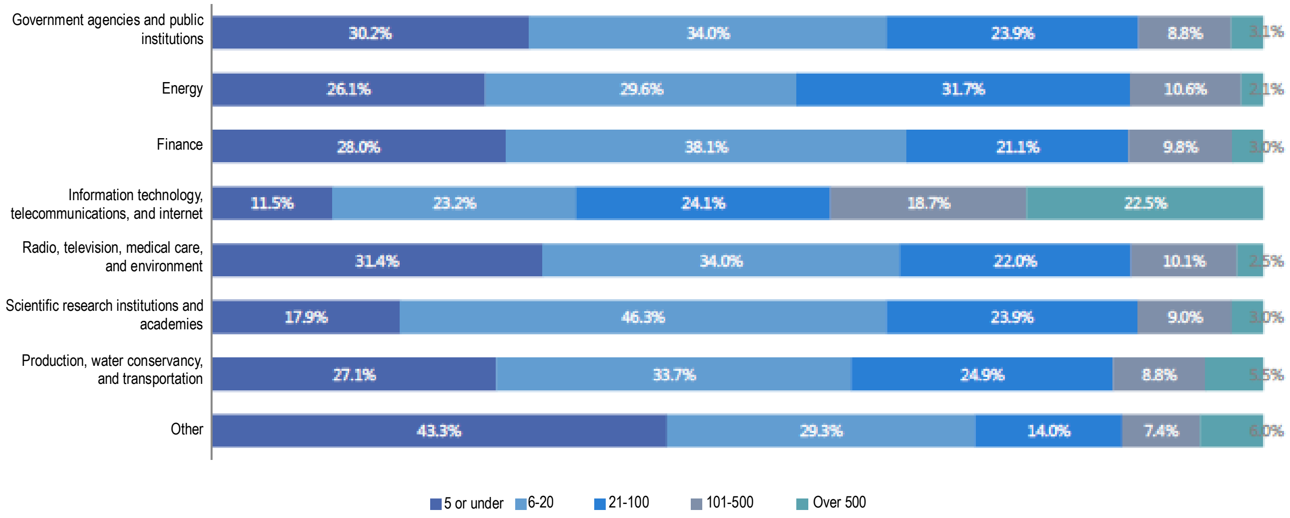


Figure 3-2 Information security team size, by industry (sample size: 4,349)

2. The larger the unit, the greater the number of information security team members

The data from this study shows that the greater the number of employees at a unit, the more capable it is of increasing information security inputs, with corresponding increases in internal information security team size (see Figure 3-3).

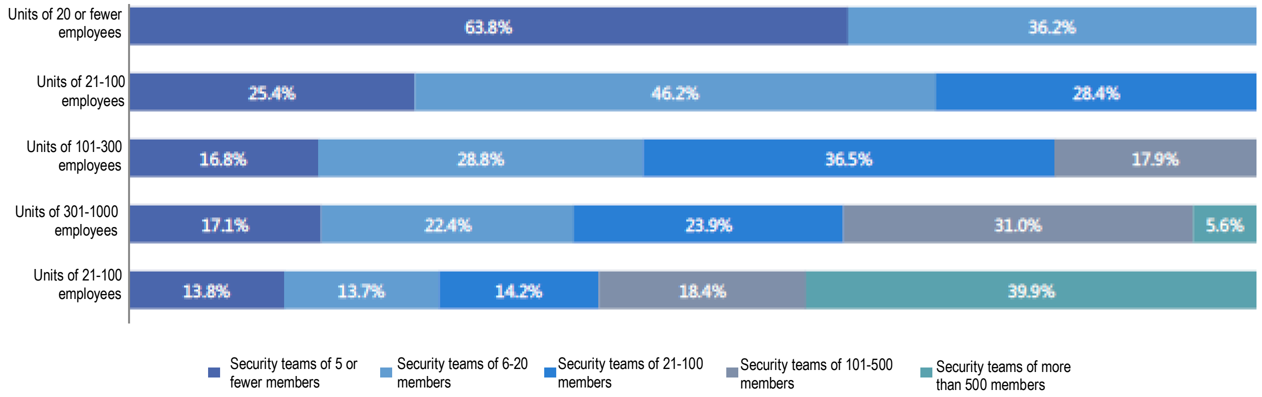


Figure 3-3 Information security team size, by unit number of employees (sample size: 4,349)

3. More than 1/3 of informatization staff are information security personnel

An overall view of the situation reveals that, on the average, personnel who were responsible for information security roles accounted for roughly 36.1% of all informatization staff. 27.3% of respondents stated that information security personnel accounted for less than 10% of informatization staff at their work units (see Figure 3-4).

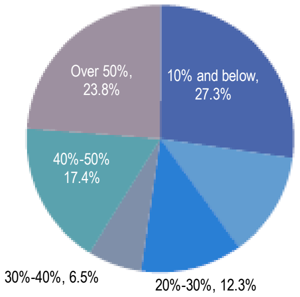


Figure 3-4 Ratio ranges of information security personnel to informatization staff (sample size: 4,349)

From the perspective of industry, we find that the ratio of information security personnel to all informatization staff was highest in the information technology, telecommunications, and internet industry: 40.8% (see Figure 3-5). Moreover, a relatively large number of respondents in this industry stated that the security personnel in their unit accounted for more than 50% (see Figure 3-6). In all other industries, the ratio of information security personnel to all informatization staff was less than the mean industry ratio (36.1%) (see Figure 3-5).

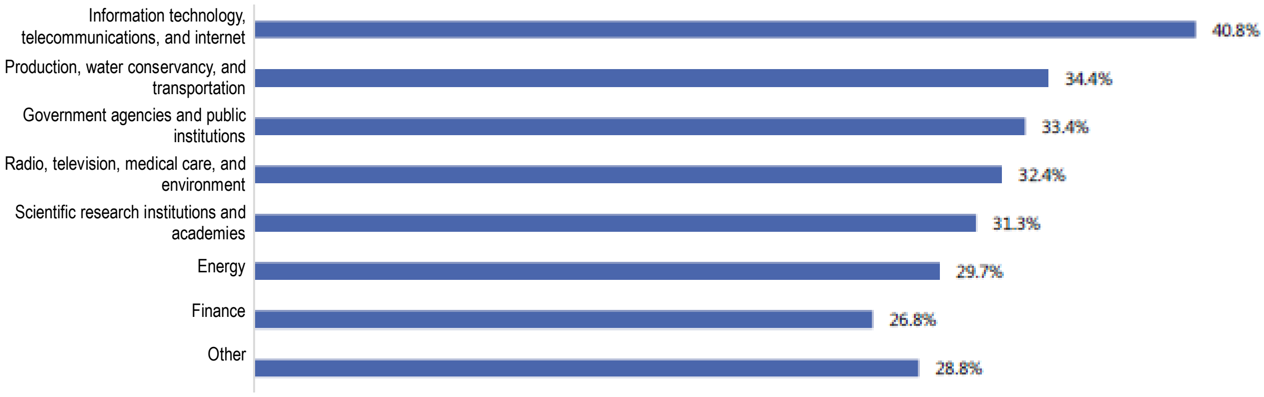


Figure 3-5 Mean ratios of information security personnel to informatization staff, by industry (sample size: 4,349)

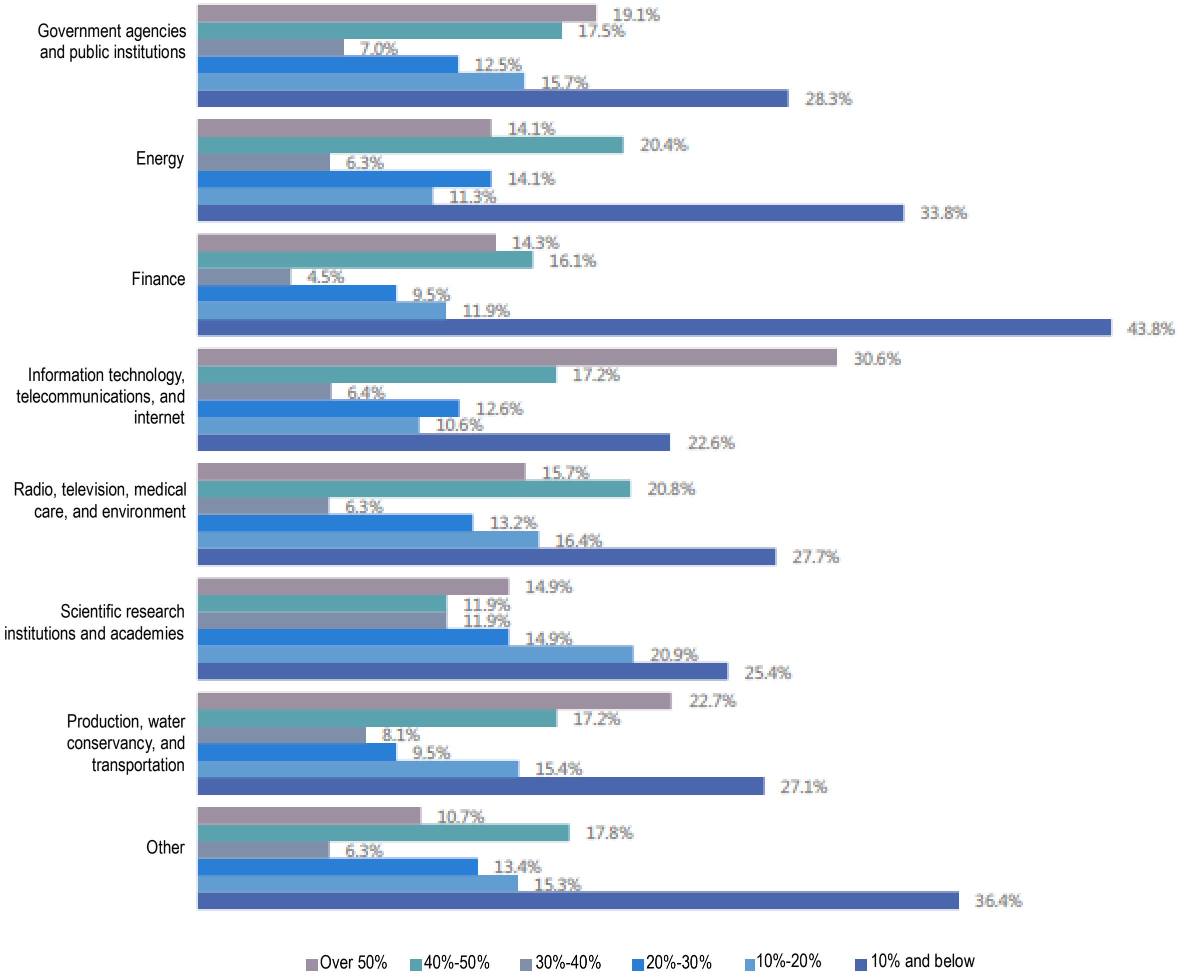


Figure 3-6 Ratio ranges of information security personnel to informatization staff, by industry (sample size: 4,349)

4. Security team size is positively related to the "security and informatization" ratio

The smaller the employer's security team, the lower is the ratio of security personnel to all informatization personnel. When employers' security teams had 5 or fewer members, the ratio of information security personnel to all informatization personnel was only 20.8%, far lower than the mean ratio (36.1%). The highest "security personnel and informatization personnel" ratio (51.2%) was found when employers' security teams had more than 500 members. This ratio was slightly higher than the mean when employers had security teams of 20-500 members (42%) (see Figure 3-7).

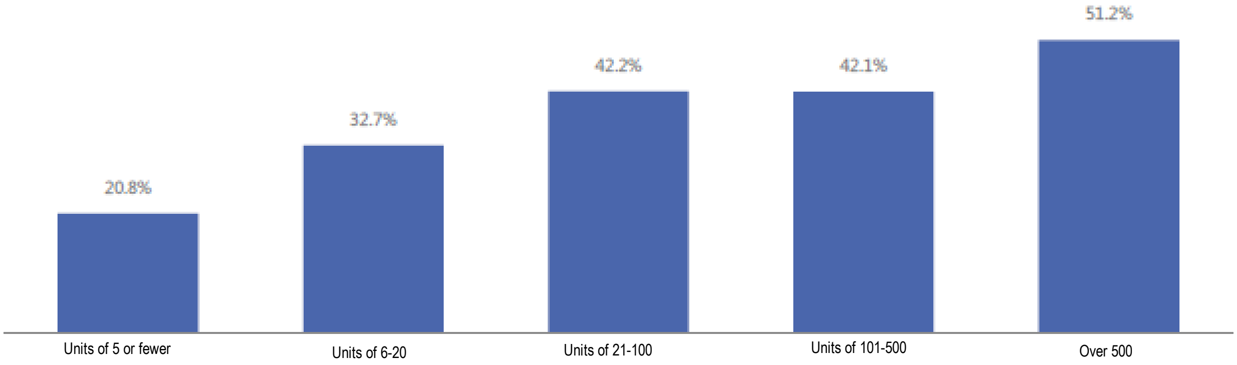


Figure 3-7 Mean ratios of information security personnel to informatization staff, by units defined according to

number of security personnel (sample size: 4,349)

II. Personnel Shortages

1. It is common for information security professionals to have to perform non-security work

Nearly sixty percent of information security professionals stated that, as a part of their jobs, they were required to do work that has no information security content (see Figure 3-8).

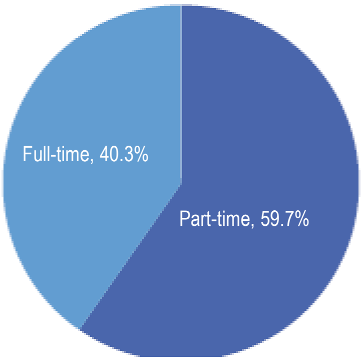


Figure 3-8 Percentages of full-time and part-time security practitioner respondents (sample size: 4,349)

The industries where the phenomenon of “one person with multiple jobs” was most pronounced among information security professionals were the following: Government agencies and public institutions (65.2%), production, water conservancy, and transportation (63.4%), energy (59.9%), and finance (58.6%) (see Figure 3-9).

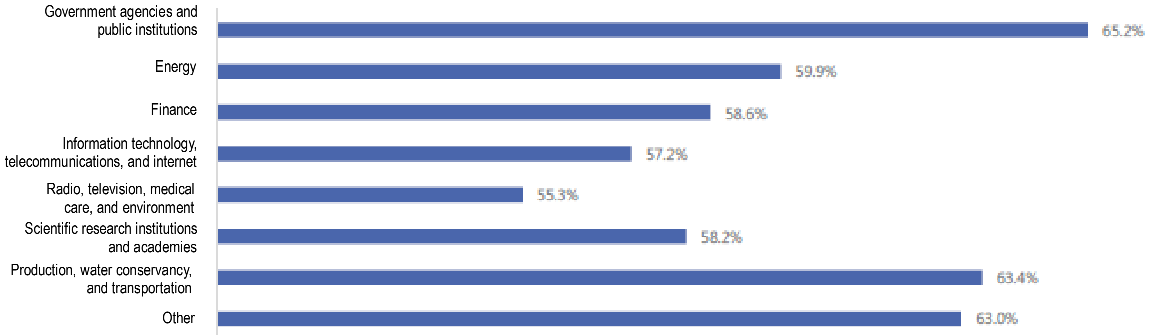


Figure 3-9 Proportion of part-time information security professionals, by industry (sample size: 2,596)

Among those who were required to additionally perform non-security work, 33.8% of respondents said that non-security work accounted for more than 50% of their everyday work (see Figure 3-10). This situation was relatively common in all industries (see Figure 3-11).

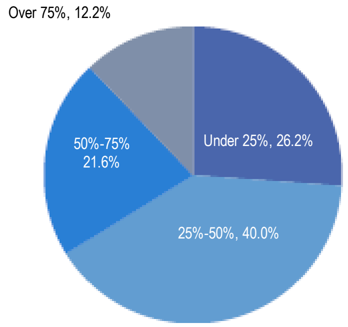


Figure 3-10 Proportion of part-time information security professionals performing non-information security work (sample size: 2,596)

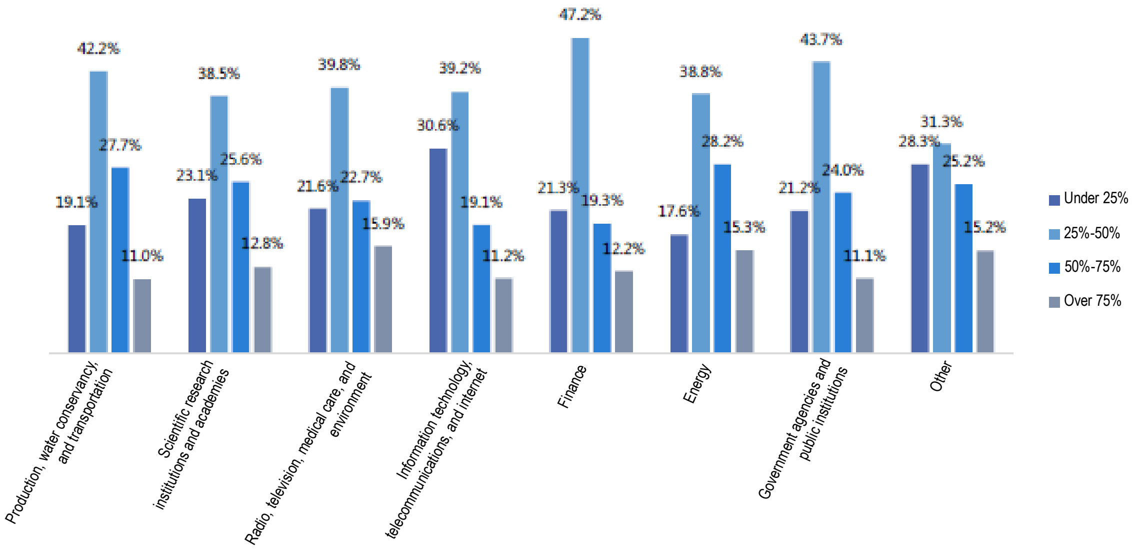


Figure 3-11 Proportion of part-time information security professionals performing non-information security work, by industry (sample size: 2,596)

2. At their current sizes, information security teams find it difficult to meet work needs

The study data shows that 46.3% of information security professionals believed that the information security team at their unit was not large enough to meet current work needs. 56.5% of information security professionals described the satisfaction of needs as “average” or “deficient” (see Figure 3-12).

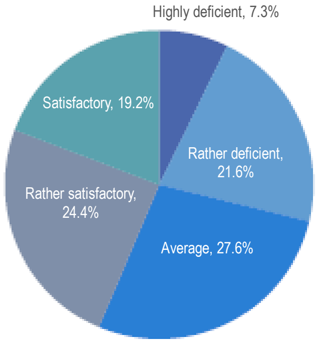


Figure 3-12 Information security teams are or are not large enough to meet current work needs (sample size: 4,349)

From the perspective of different professional work positions, we see that the high and middle ranks tended to believe the information security personnel teams in their units could meet current work needs, while project managers and entry-level professionals were more likely to perceive a shortage of information security personnel at their units (see Figure 3-13).

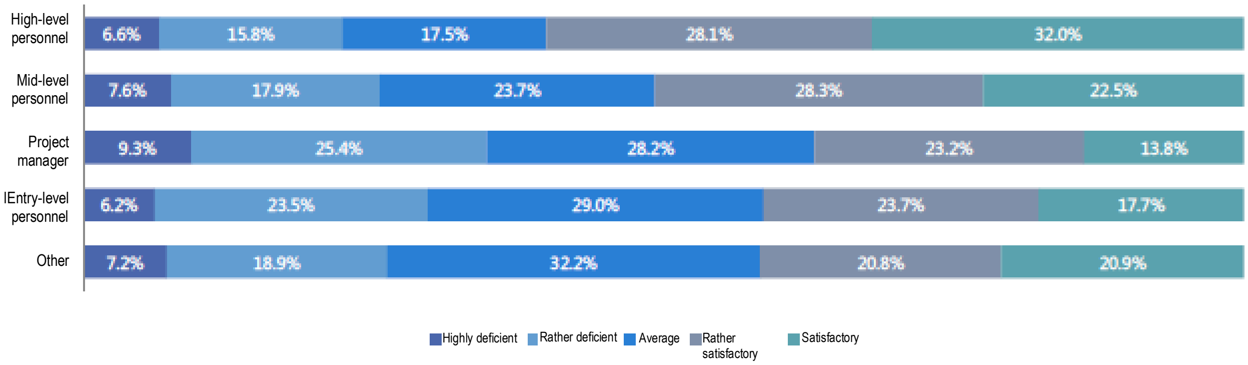


Figure 3-13 Practitioners' evaluations of unit security personnel shortages, by work position (sample size: 4,349)

In addition, part-time information security professionals have an even more obvious perception of security personnel shortages. Among part-time practitioners, 9.5% of respondents believed that the supply of security personnel was highly deficient. This figure was double that of full-time practitioners. Merely 37.2% of part-time personnel believed that the number of security personnel was rather satisfactory, but 51.6% of full-time practitioners believed that work needs could be met (see Figure 3-14).

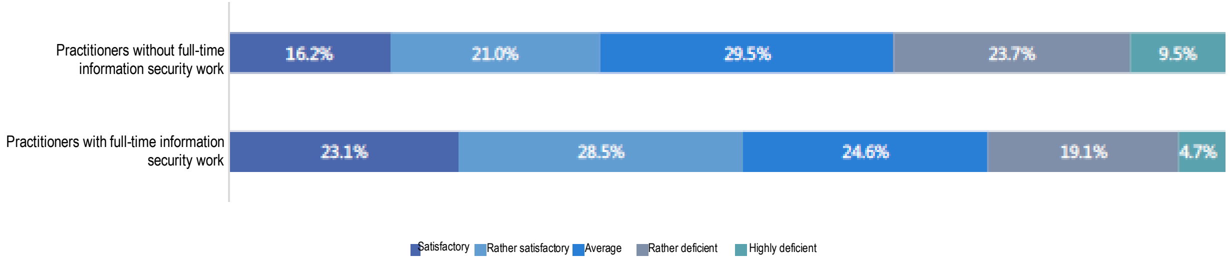


Figure 3-14 Part-time and full-time professionals' evaluations of unit security personnel shortages (sample size: 4,349)

3. The shortage of information security personnel may add to practitioner work stress

The data shows that the more severe the shortage of information security personnel, the greater is the work stress of professionals. When the number of security personnel at a work unit was highly deficient, 43.1% of professionals said they experience relatively severe work stress, and 24.1% believed that their work stress was very severe. When their work unit had enough security personnel to meet work needs, professionals experienced significantly less stress. Only 29.5% of such respondents felt that their work stress was relatively severe and fewer than 5% felt that it was very severe (see Figure 3-15).

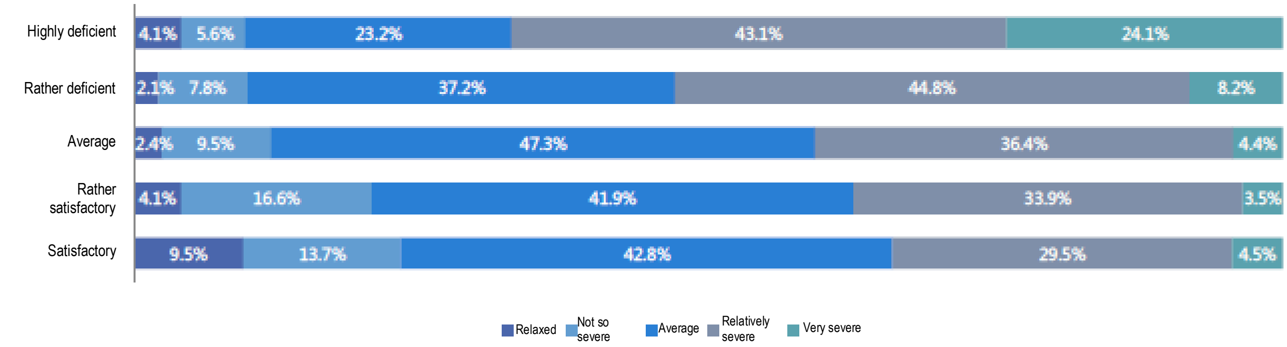


Figure 3-15 Respondent perception of work stress, by degree of security personnel shortage (sample size: 4,349)

4. Talent shortages are even more pronounced in the planning and management and security development work roles

Respondents believed that shortages existed for all types of information security work roles, with the severest shortages occurring among the following work roles: The analysis design (35.9%) and development and integration (30.5%) subcategories within the "security development" category, the strategic planning (27.6%) and organizational management (33.5%) subcategories in the "planning and management" category, and the formulation of strategies and regulations (25.3%) and information security enforcement and regulation (24.6%) subcategories in the "regulatory governance" category.

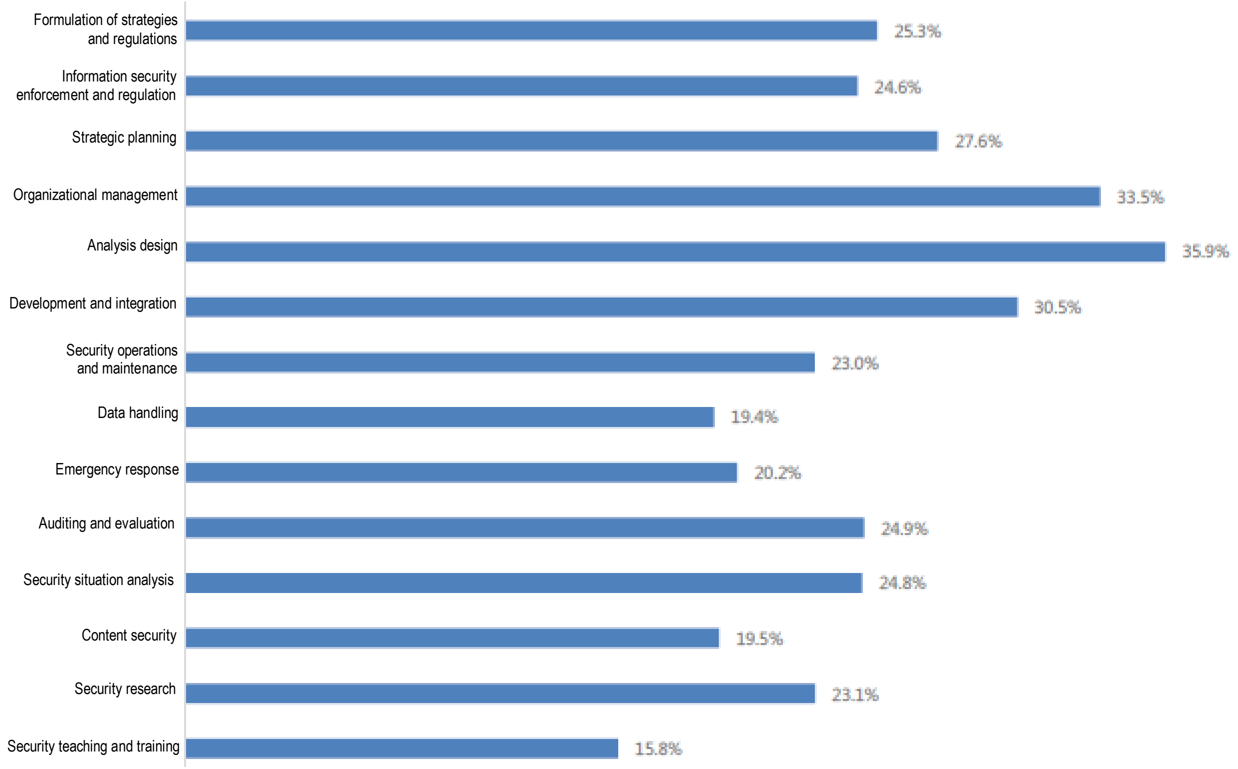


Figure 3-16 Types of information security talent shortages (sample size: 4,349)

4. Mobility and Allocation

As society's process of informatization continually accelerates and the cybersecurity situation grows increasingly complex, cyber and information security professionals have become “inelastic demand-type” talent for all kinds of units and organizations. In 2018, it was estimated that China’s cybersecurity industry would reach RMB 54.549 billion, a 25.1% increase over the previous year.[4] With the rapid development and expansion of the cyber and information security industries, the demand for information security professionals underwent further growth, and the problem of talent supply-demand imbalance persisted.

Critical information infrastructure (关键信息基础设施) serves as the “central nervous system” for the functioning of the economy and society. It is thus necessary to fully assure the supply of security talent. However, the study shows that a large number of critical information infrastructure operators are facing challenges in the areas of attracting talent, employing talent, and retaining talent. Talent loss is severe. Information security is a non-traditional security field, and information security occupations are classified as non-traditional occupations. To spur the flow of information security professionals to important industries and critical information systems, we need to conduct an in-depth investigation of trends and characteristics of security talent occupational mobility and then formulate innovative solutions. In this chapter, the study mainly proceeds in respect to the three areas of salary level, occupational satisfaction, and occupational mobility in order to gain an understanding of the current mobility and allocation situation of information security professionals.

I. Salary Levels

II. Occupational Satisfaction

III. Occupational Mobility

[4] [Translation of footnote in the Chinese source text] China Academy of Information and Communications Technology (CAICT): White Paper on China's Cybersecurity Industry (2018).

Salary Levels

This study shows that the average annual salary of an information security practitioner in China was RMB 150,300, which was higher than the average income level in information technology-related industries. Information security practitioner salaries continued to climb relative to the previous year, but the magnitude of the increase declined. The proportion of personnel whose salary increased by more than 10% significantly decreased. The industry with the highest mean salary for information security professionals was the finance industry (RMB 200,000). The lowest was government agencies and public institutions (RMB 136,000). The level of salary satisfaction among practitioners basically held steady relative to the previous year, but the number of dissatisfied people rose slightly. Association analysis shows that the mean annual salary of practitioners with cybersecurity competition experience (RMB 170,000) was significantly higher than for those without competition experience (RMB 148,000).

Occupational Satisfaction

42.9% of information security professionals stated that work stress was “relatively severe” or “very severe,” which represented a decline relative to the previous year. Overtime is a common phenomenon in the information security industry. More than eighty percent of practitioners experienced varying degrees of overtime. Nearly a third of respondents had more than 10 hours overtime per week. 51.2% of information security professionals expressed “average” satisfaction with their work position. The proportion of practitioners satisfied with their work position (32.7%) was significantly higher than the proportion of practitioners who were dissatisfied (16.2%.) Overall, although the impression of work stress was quite apparent among practitioners, respondent satisfaction with salary and work position remained positive overall, and the majority were optimistic about their prospects for career development.

Occupational Mobility

The reasons that information security professionals gave for choosing to enter this industry were, in order of importance: “Favorable assessment of career development prospects,” “interest or hobby,” “professional match,” and “security mission and self-realization of values.” Practitioners’ intrinsic motivations had a relatively large effect on the reasons; “remuneration” was ranked fifth. As for the reasons affecting practitioners’ further occupational mobility, they were, in order of importance: “Salary,” “opportunities for promotion,” “work atmosphere,” and “self-realization of values.” This indicates that when practitioners switch to new employers they attach great importance to both benefit and development-related factors. There was a decline relative to the previous year in the percentage of practitioners who changed work units during the past three years, and the percentage of those who did not experience occupational mobility rose. The rate of talent mobility has slowed. In addition, the two factors that employers value the most when recruiting information security talent are: Whether candidates have information security credentials and whether they have related job experience.

I. Salary Levels

1. The overall salary levels of practitioners continued to climb

The study data shows that the average annual salary of an information security practitioner in China was RMB 150,300, which was higher than the 2018 average income level of RMB 142,000 in information technology-related industries as published by the National Bureau of Statistics.[5] The average annual salary of more than half of practitioners (53.4%) was in the RMB 100 to 200 thousand range (see Figure 4-1.)

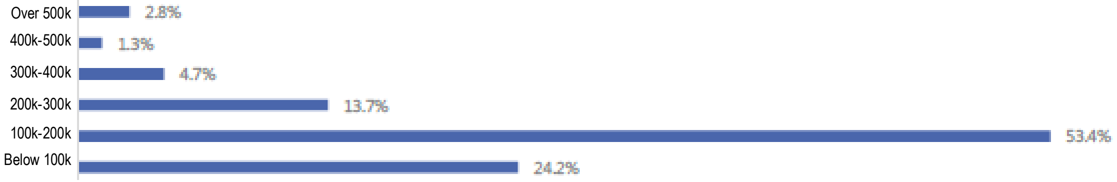


Figure 4-1 Respondent salaries (sample size: 4,347)

The percentage of practitioners with an annual salary less than RMB 100,000 declined to 24.2% from 41.6% in the previous year. All population segments with annual salaries above RMB 100,000 rose relative to the previous year (see Figure 4-2.)

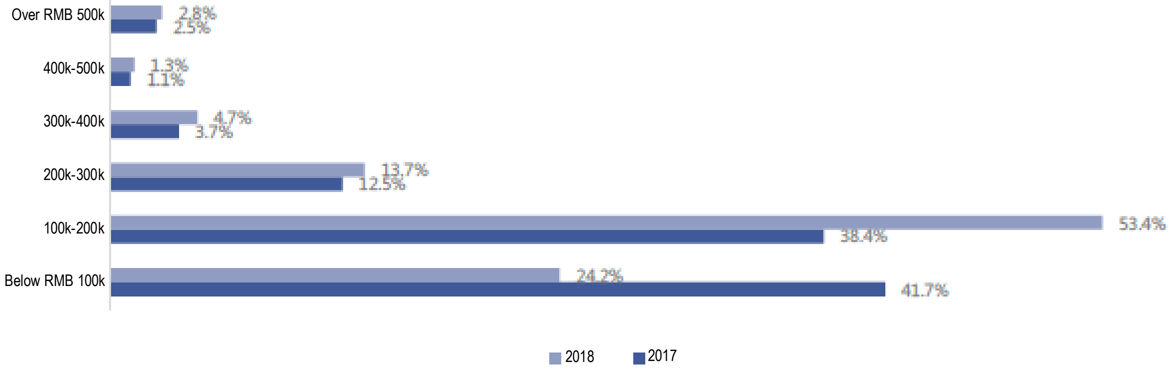


Figure 4-2 Respondent salaries, 2017 vs. 2018

From the perspective of industry, the highest mean annual salary for information security professionals was in the finance industry, where it was approximately RMB 200,000. The next two highest-paying industries were the production (生产) | water conservancy | transportation industry, and the energy industry, with RMB 163,000 and RMB 157,000, respectively. The industries with the lowest mean annual salary were the radio, television | environmental protection | public health and medicine sector, and government agencies and public institutions, with RMB 142,000, and RMB 136,000, respectively. The mean annual salary in the information technology, telecommunications, and internet industry, where information security professionals are concentrated, was RMB 155,000, slightly higher than the national average (RMB 153,000.) In

[5] [Translation of footnote in the Chinese source text] National Bureau of Statistics *2018 Annual Mean Wages of Personnel Employed by Enterprises Above the Designated Size Broken Out by Job*: The mean annual salary of all persons employed in the "information transmission, software, and information technology services industry" was RMB 141,962.

scientific research institutes and institutions of higher learning, which have the lowest proportion of information security professionals, the mean annual salary was RMB 150,000, slightly lower than the national average (see Figure 4-3.)

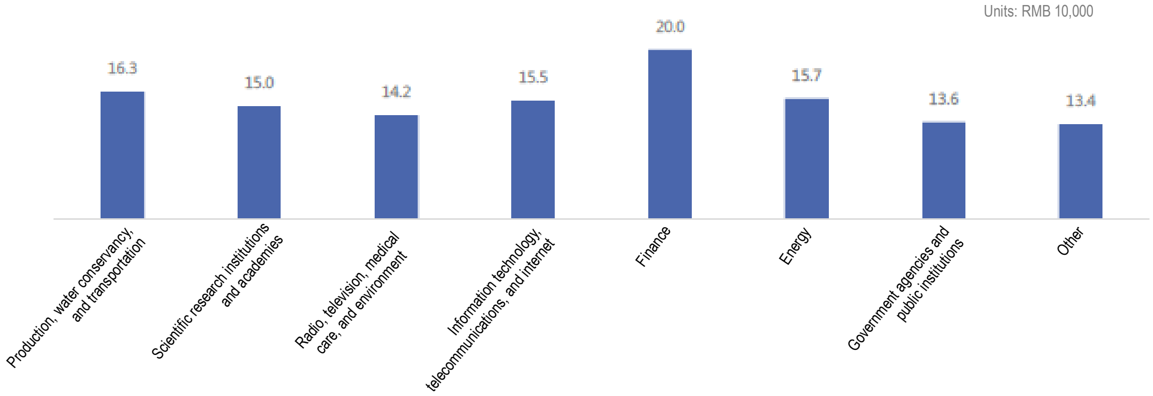


Figure 4-3 Respondent mean annual salaries, by industry (sample size: 4,347)

2. Salary was positively related to educational background and years of employment

The sample data indicates that, overall, the more education an information security practitioner has, the higher the mean annual salary (see Figure 4-4.)

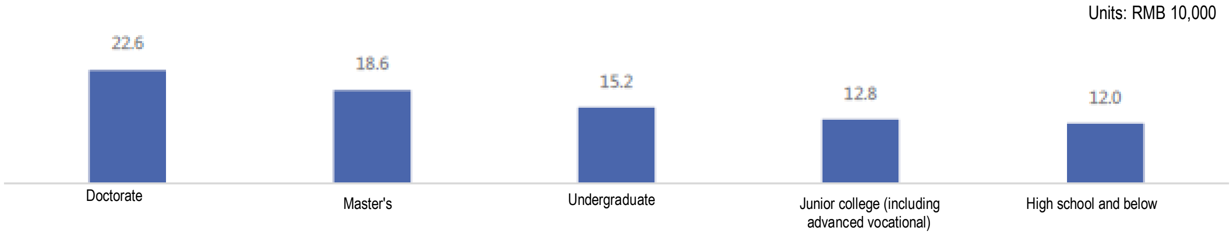


Figure 4-4 Respondent mean annual salaries, by educational background (sample size: 4,347)

Practitioners with a doctoral degree had the highest proportion of high-income earners. The lowest proportion of high-income earners was found among practitioners with a junior college degree (see Figure 4-5.)

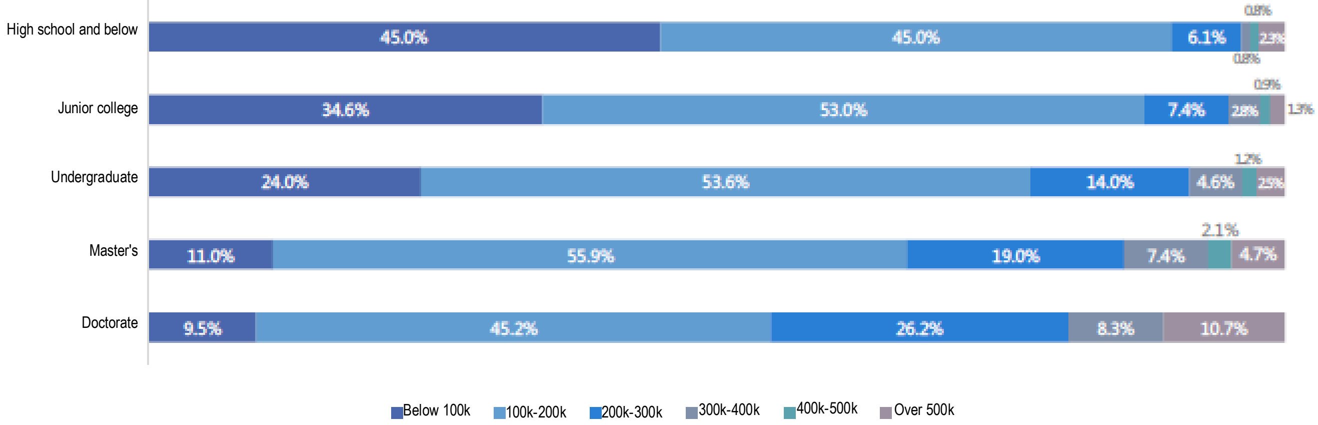


Figure 4-5 Salary brackets, by educational background (sample size: 4,347)

Shorter periods of employment correlated with lower salaries. Practitioners who had worked for less than one year had the lowest mean annual salary, just RMB 106,000. Respondents with 11-20 years of employment had the highest annual salaries; their mean annual salary was RMB 221,000 (see Figure 4-6.)

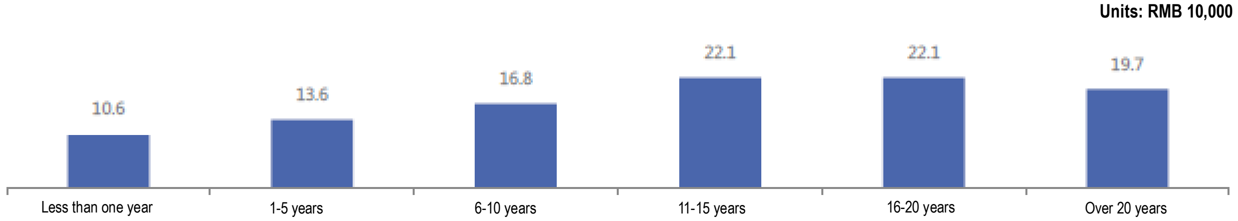


Figure 4-6 Respondent mean annual salaries, by years of work (sample size: 4,347)

However, the positive relationship between salary and years of employment ceases to hold for practitioners with more than 15 years of employment, and a polarization trend appears (see Figure 4-7.)

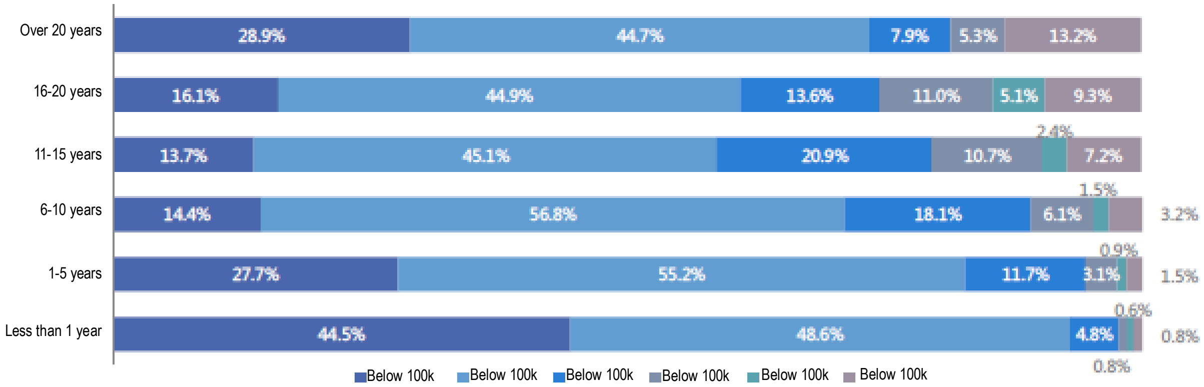


Figure 4-7 Respondent annual salary brackets, by years of work (sample size: 4,347)

3. The amount of increase in overall salaries declined relative to the previous year

The study data shows that nearly sixty percent (57.5%) of information security professionals saw increases of varying degrees over their prior year salaries. Those with an increase under 5% accounted for the highest proportion, 26.2% (see Figure 4-8).

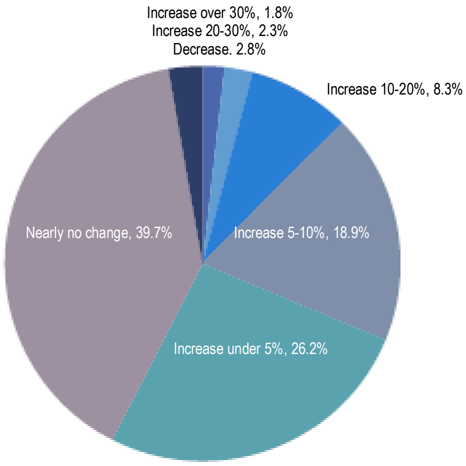


Figure 4-8 Change to respondents' prior year salaries (sample size: 4,349)

The amount of increase in overall practitioner salaries declined relative to the previous year. There was a significant decrease in the percentage of professionals who saw a salary increase in excess of 10% (see Figure 4-9).

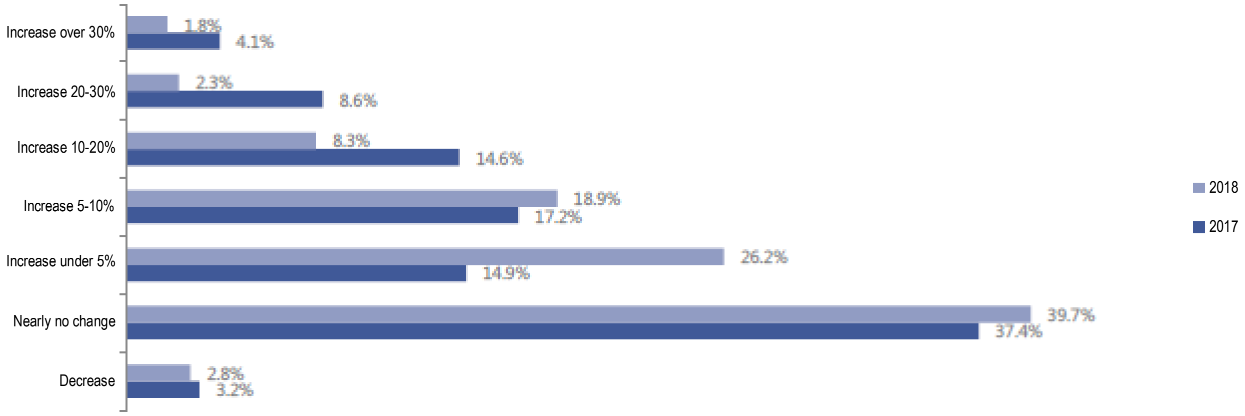


Figure 4-9 Change in respondent past-year salaries, 2017 vs. 2018

From the perspective of work roles, we find that salary increases in excess of 10% accounted for relatively high proportions of those performing the planning and management, scientific research and education, and security development categories of work roles (see Figure 4-10). Among those in the planning and management and security operations work role categories, the percentage who saw a salary increase over the previous year increased by 8.5 percentage points, but the percentage of those in the regulatory governance work role who saw a salary increase over the previous year declined by 12.2 percentage points.

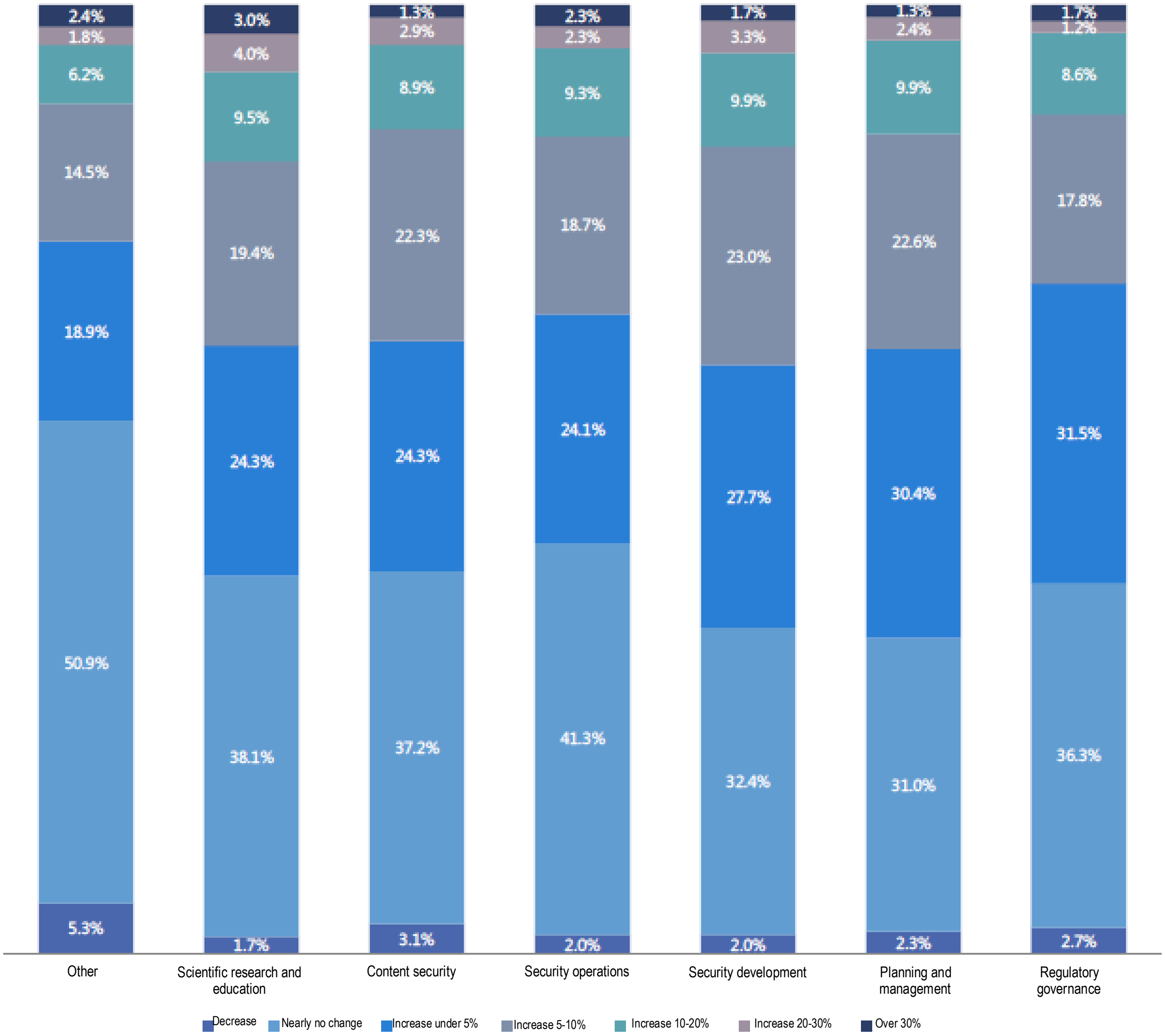


Figure 4-10 Change in past-year respondent salaries, by work role (sample size: 4,349)

4. The level of salary satisfaction among professionals was similar to the previous year

The study data indicates that 48.7% of information security professionals had an “average” level of satisfaction regarding salary. Practitioners who were dissatisfied with their salary accounted for 27.4%, slightly higher than the satisfied population (24%) (see Figure 4-11).

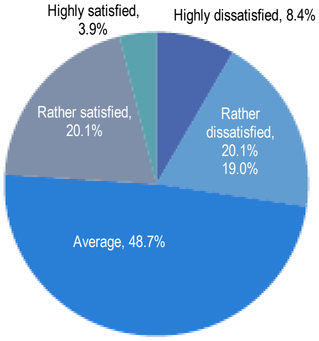


Figure 4-11 Level of practitioner salary satisfaction (sample size: 4,349)

The satisfied population basically held steady relative to the previous year (23.4%). However, there was a slight increase in the dissatisfied population, 3.2 percentage points higher than the previous year (24.2%). The overall level of salary satisfaction differed little from the previous year. An examination according to industry shows that, among practitioners at scientific research institutions and academies, 39.4% of respondents expressed satisfaction with their current salary, significantly higher than other industries (see Figure 4-12).

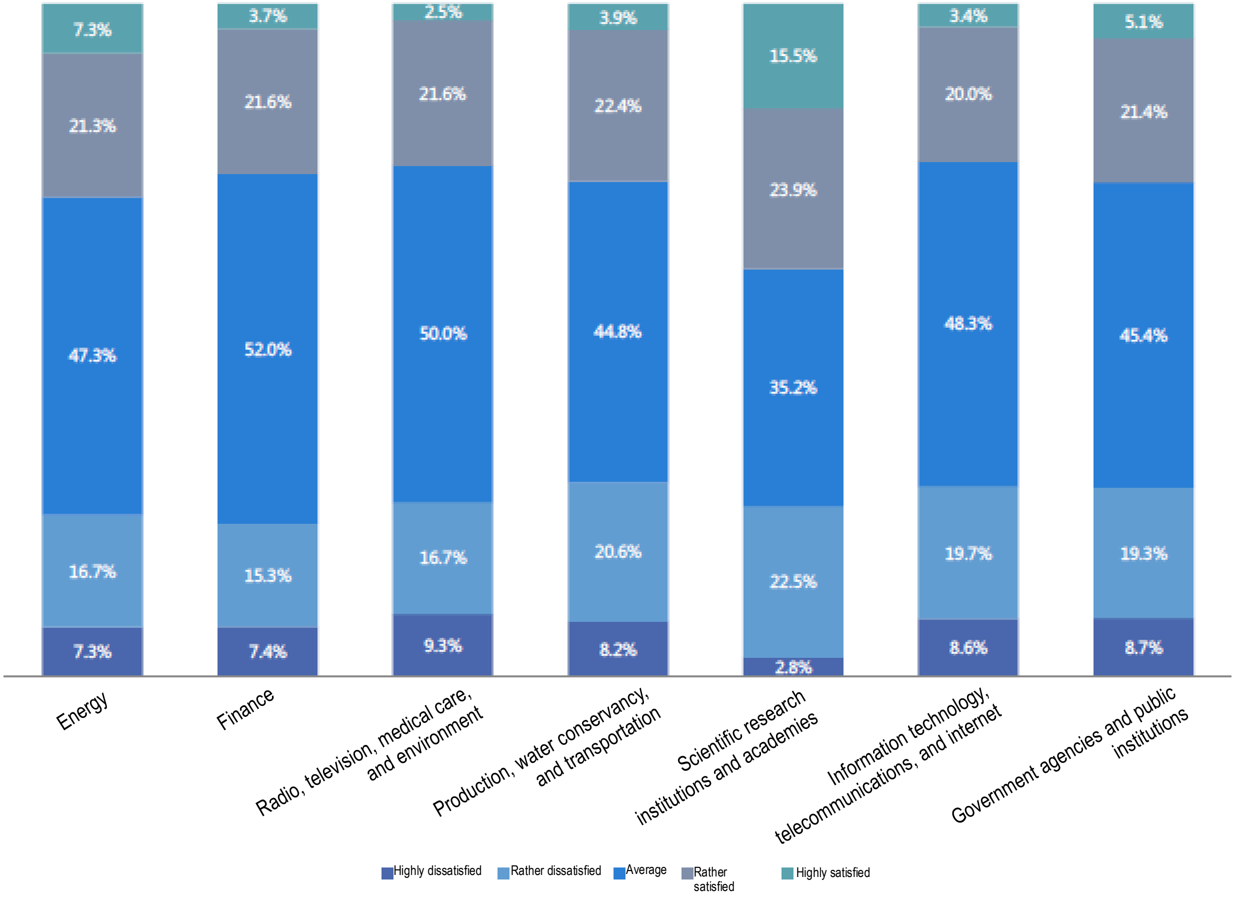


Figure 4-12 Respondent salary satisfaction, by industry (sample size: 4,349)

5. Practitioners with competition experience had higher salaries

Association analysis of information security practitioner competition experience vis-à-vis salary shows that the mean annual salary of practitioners who participated in cybersecurity competitions in China (RMB 170,000) was significantly higher than for those without competition experience (RMB 148,000) (see Figure 4-13).

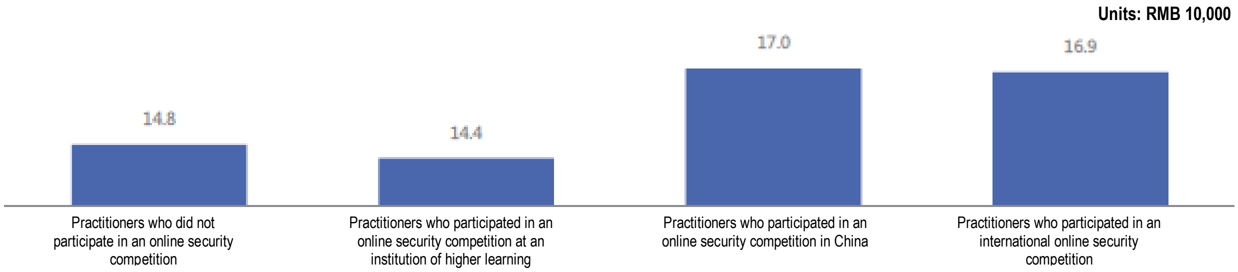


Figure 4-13 Practitioner mean annual salaries, by participation in type of online security competition (sample size: 4,347)

II. Occupational Satisfaction

1. There was a relatively obvious perception of stress among practitioners overall

Information security professionals had a relatively obvious perception of work stress. 42.9% of practitioners perceived their work stress to be "relatively severe" or "very severe." Only 15.9% of practitioners perceived their work stress to be "not so severe" or "relaxed" (see Figure 4-14).

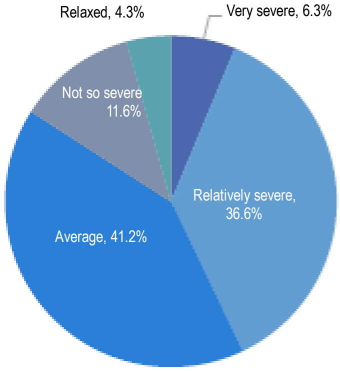


Figure 4-14 Respondent work stress (sample size: 4,349)

However, relative to the previous year's data (53.7%), there was a decline in the proportion of practitioners who perceived their work stress as "relatively severe" or "very severe" (see Figure 4-15).

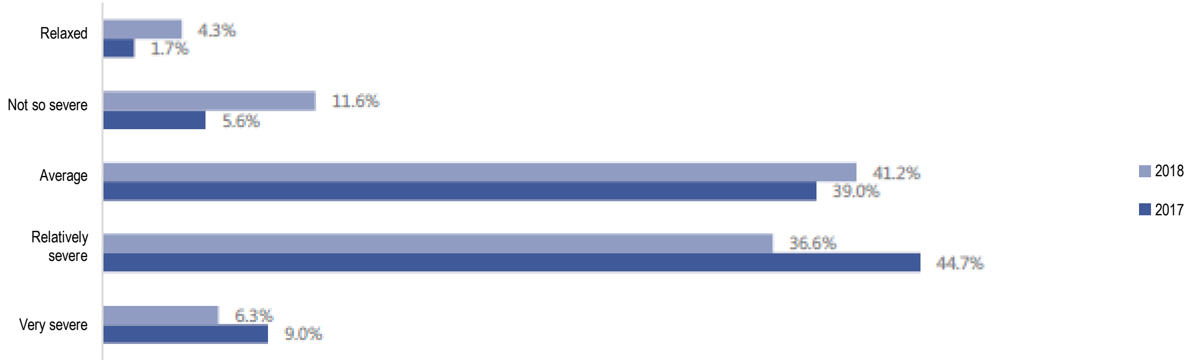


Figure 4-15 Respondent work stress, 2017 vs. 2018

The main industry in which perceptions of work stress were most obviously concentrated was the information technology, telecommunications, and internet industry, where 49.2% of practitioners regarded the stress as "relatively severe" or "very severe." In other industries, the proportions of practitioners with relatively severe work stress were lower than the mean proportion nationally. Information security professionals at scientific institutions and academies had the lowest work stress. Only 20.9% of these practitioners had "relatively severe" or "very severe" stress (see Figure 4-16).

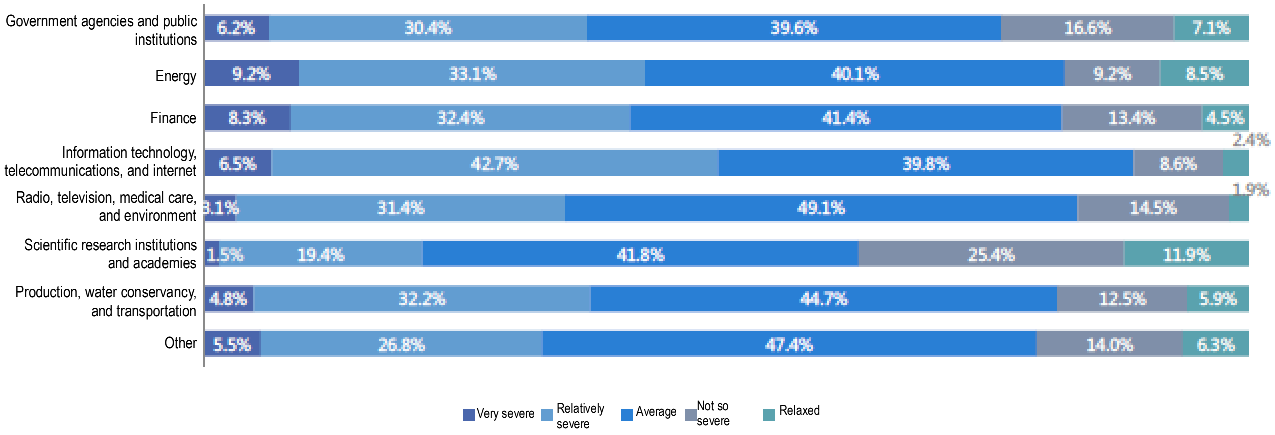


Figure 4-16 Respondent work stress, by industry (sample size: 4,349)

From the perspective of work unit nature, the most severe work stress was perceived by private enterprise information security professionals: 47.0% of them perceived their work stress as "relatively severe" or "very severe," significantly higher than the national mean (42.9%). Only 12.0% of such practitioners perceived their work stress as "not so severe" or "relaxed," slightly less than the national mean (15.9%) (see Figure 4-17).

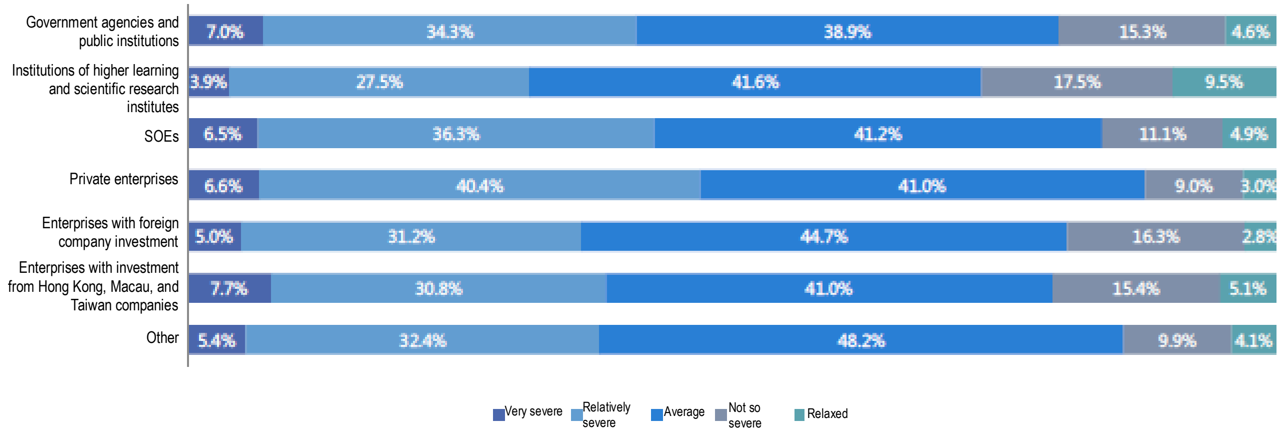


Figure 4-17 Respondent work stress, by work unit nature (sample size: 4,349)

2. The practice of overtime was widespread, but the "overtimers" had higher salaries

The study data indicates that more than eighty percent of information security professionals experienced varying degrees of overtime (see Figure 4-18). 49.9% of practitioners had 10 or fewer hours of overtime per week, and 32.7% had more than 10 hours of overtime per week (see Figure 4-18).

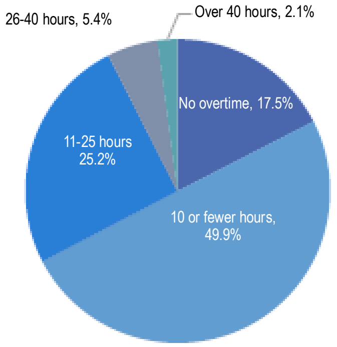


Figure 4-18 Respondent weekly overtime (sample size: 4,349)

In addition, the amount of overtime was positively related to mean salary. The mean annual salary of practitioners with more than 40 hours of overtime per week was more than twice that of practitioners with no overtime and 1.5 times higher than the mean annual salary of practitioners with 26-40 hours overtime per week (see Figure 4-19).

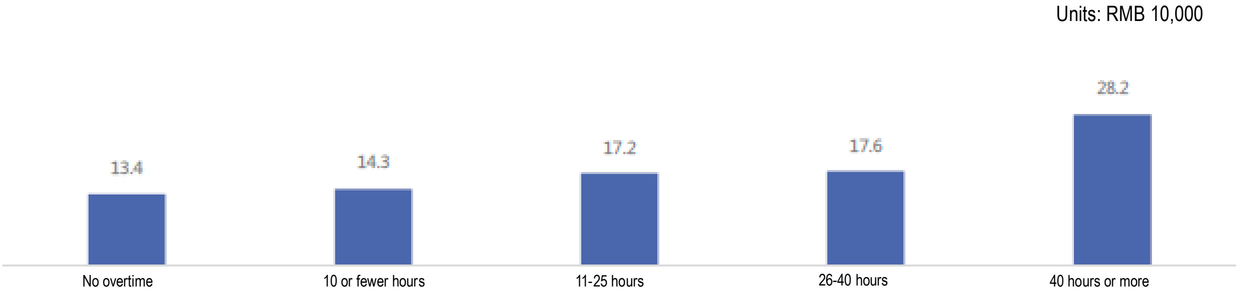


Figure 4-19 Respondent mean annual salary, by amount of overtime (sample size: 4,347)

From the perspective of industry, we see that the proportions of practitioners with weekly overtime in energy, information technology, telecommunications and internet, and in production, water conservancy, and transportation were higher than the national average and that the proportions of practitioners with weekly overtime in government agencies and public institutions, radio and television, public health and medicine, environmental protection, scientific research institutions and academies, and other industries were lower than the national average. Practitioners with more than 10 hours overtime per week were mainly distributed across the energy, information technology, telecommunications, and internet; production, water conservancy, and transportation; and finance industries (see Figure 4-20).

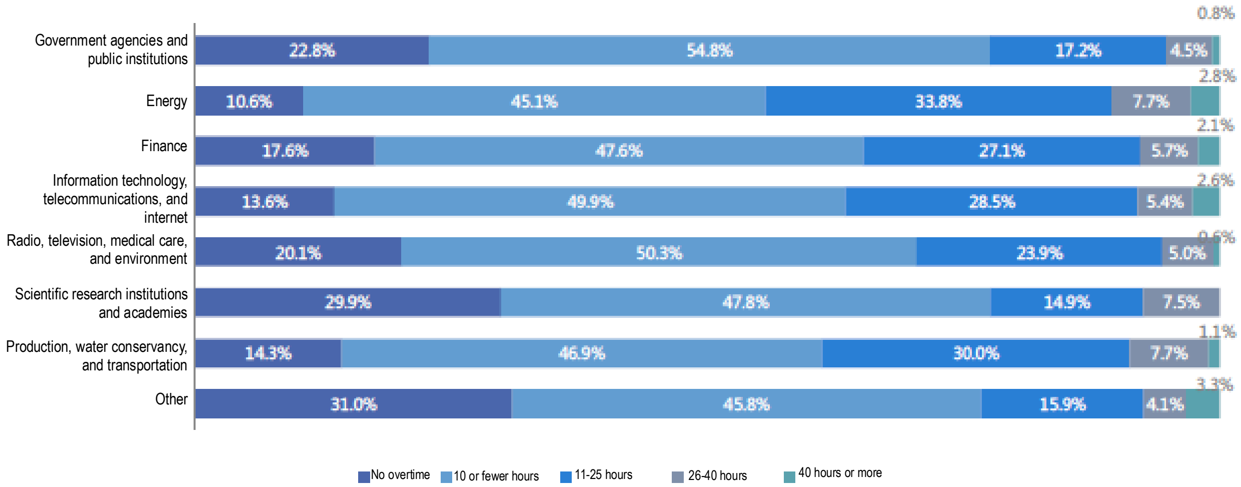


Figure 4-20 Respondent weekly overtime, by industry (sample size: 4,349)

From the perspective of work unit nature, we see that, overall, the proportion of information security professionals with weekly overtime in government agencies and public institutions, enterprises with foreign investment, and institutions of higher learning and scientific research institutes was lower than the national average. Overall, the proportion of information security professionals with weekly overtime in enterprises with Hong Kong, Taiwan, and Macau investment and in private enterprises was significantly higher than the national average. Among the former, 46.2% of practitioners had 11-25 hours of weekly overtime. 49.7% of practitioners had 10 or fewer hours of weekly overtime in the latter group. Units which had a higher proportion of practitioners with more than 10 hours overtime per week included enterprises with Hon Kong, Taiwan and Macau investment, private enterprises, institutions of higher learning and scientific research institutes, and SOEs. The proportions there were 59.0%, 35.2%, 34.1% and 33.8%, respectively, all higher than the national average (see Figure 4-21).

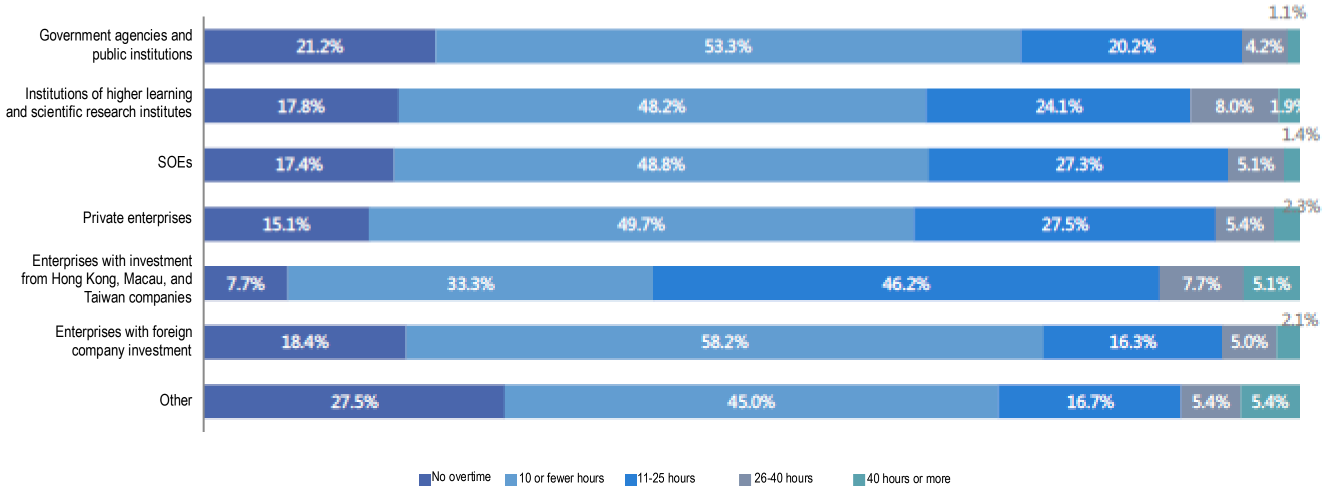


Figure 4-21 Respondent weekly overtime, by unit nature (sample size: 4,349)

3. The level of satisfaction with work position declined, but was positive overall

The study data indicates that 51.2% of information security professionals expressed "average" satisfaction with their work position. However, the proportion of practitioners satisfied with their work position (32.7%) was significantly higher than the proportion of practitioners who were dissatisfied (16.2%) (see Figure 4-22). The proportion of the study population with "average" occupational satisfaction increased by 2.1 percentage points over the previous year. However, the proportion of practitioners who were satisfied with their work position dropped 5.7 percentage points.

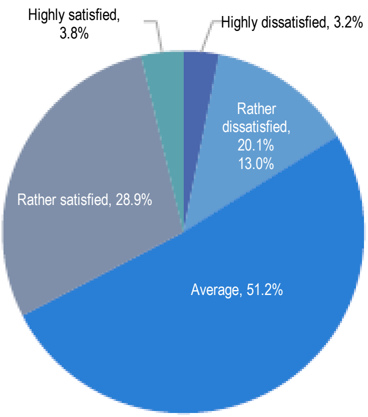


Figure 4-22 Respondent work position satisfaction (sample size: 4,349)

From the perspective of industry, we see that the study population with higher work position satisfaction was mainly distributed in the information technology, telecommunications, and internet industry. The proportion of practitioners in this industry that were more satisfied with their work position (35.6%) was significantly higher than the proportion of practitioners who were more dissatisfied (14%). The work position satisfaction of information security professionals in the energy and other (non-categorized) industries was not very high. In the two industries mentioned above, the proportions of practitioners who had more work position satisfaction (24.6% and 16.4%, respectively) were not very different from the proportions of practitioners who had more work position dissatisfaction (28.2% and 19.5%, respectively) (see Figure 4-23).

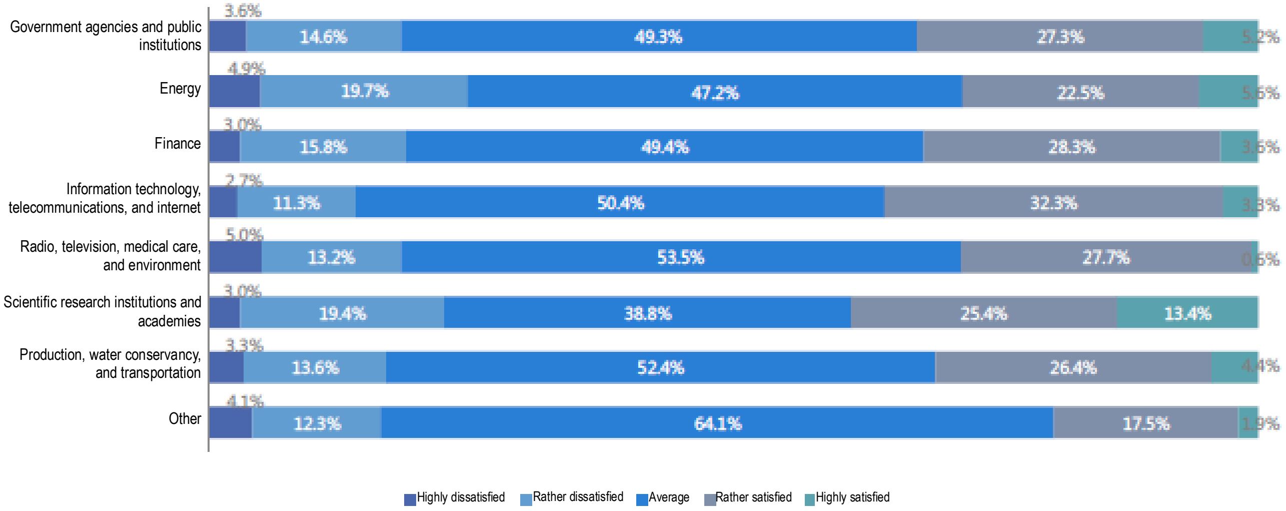


Figure 4-23 Respondent work position satisfaction, by industry (sample size: 4,349)

From the perspective of work unit nature, we find that the proportion of information security professionals in all enterprises and public institutions satisfied with their work position was significantly higher than those who were dissatisfied. The work position satisfaction of information security professionals in enterprises with foreign investment, private enterprises, and institutions of higher learning and scientific research institutes was higher than that of practitioners in SOEs and government agencies and public institutions (see Figure 4-24).

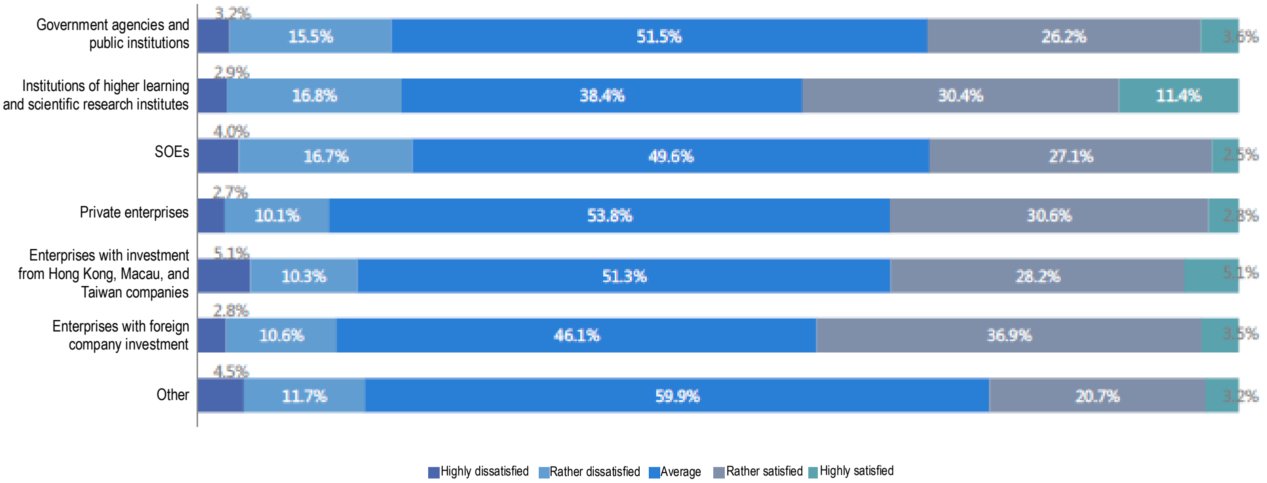


Figure 4-24 Respondent work position satisfaction, by work unit nature (sample size: 4,349)

III. Occupational Mobility

1. Favorable assessment of career development prospects was the primary reason for entering the industry

The main reasons that information security professionals engage in security work were, in order of importance: “Favorable assessment of career development prospects,” “interest or hobby,” "professional match," and "security mission and self-realization of values." As informatization developed and the Chinese state gradually began taking cybersecurity more seriously in recent years, "favorable assessment of career development prospects" in the information security industry replaced the previous year's "interest or hobby" as the primary reason that information security professionals gave for engaging in security work. "Remuneration" ranked only fifth. This ranking was the same as the survey result of the previous year. It still was not a primary reason for choosing to enter the security industry (see Figure 4-25).

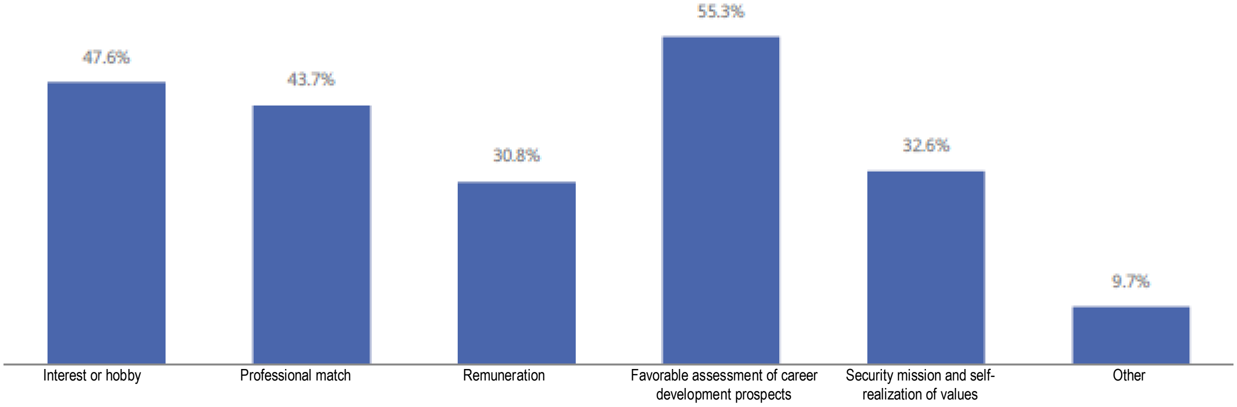


Figure 4-25 Primary reasons practitioners have for engaging in security work (sample size: 4,349)

2. More than 1/3 of practitioners experienced job changes during the past three years

During the past three years, a total of 35.9% of information security professionals switched to a new work unit. 64.1% of information security professionals did not experience a job change, a slight increase over the previous year figure (59.9%). 32.0% of the study population switched work units 1-2 times, a 5.3 percentage point drop relative to the previous year (37.3%). The rate of talent mobility has slowed (see Figure 4-26).

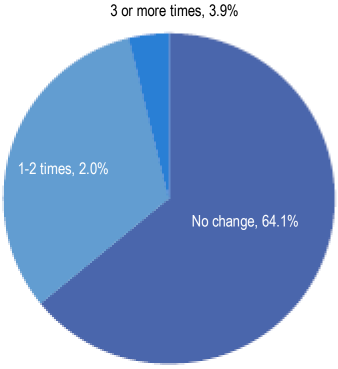


Figure 4-26 Respondent job change frequency over the past three years (sample size: 4,349)

At the same time, the sample data of this study shows that the proportion of practitioners with definite, recent job change intentions was roughly 16.4%, while 56.1% of practitioners indicated they would not change jobs (see Figure 4-27).

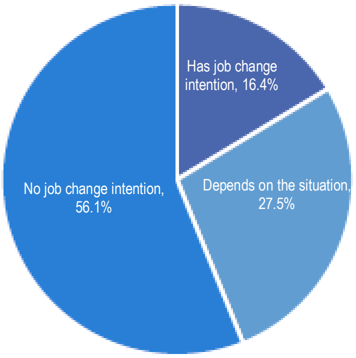


Figure 4-27 Respondent job change intentions (sample size: 4,349)

3. Salary and opportunities for career advancement were the main reasons for talent mobility

The study data shows that salary and opportunities for advancement were the main factors affecting occupational mobility among information security professionals (see Figure 4-28).

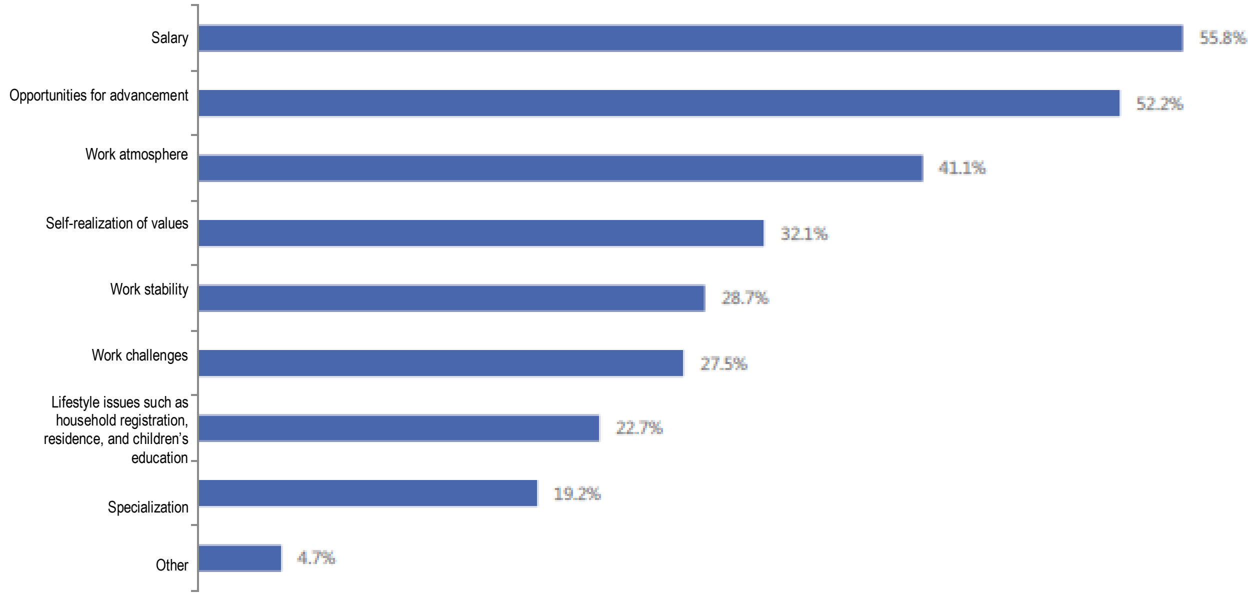


Figure 4-28 Reasons for information security talent mobility (sample size: 4,349)

According to data analysis, the higher the level of salary satisfaction of practitioners, the lower their job change intention. 90% of respondents who were highly satisfied with their salaries stated that they did not plan to change jobs (see Figure 4-29).

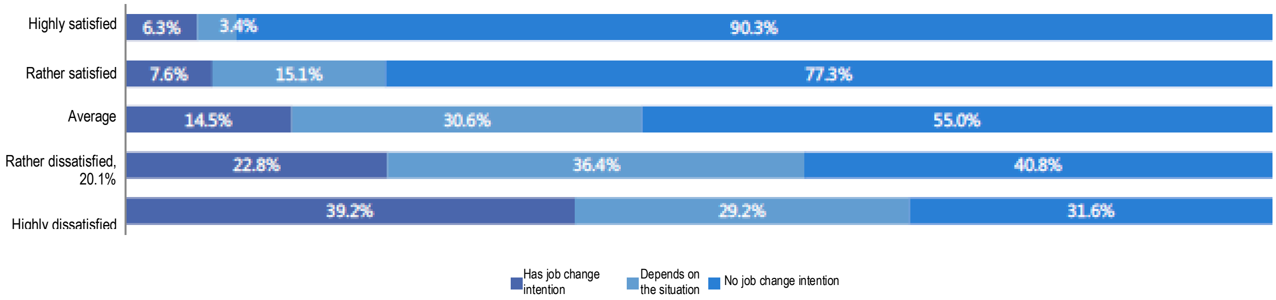


Figure 4-29 Respondent job change intentions, by salary satisfaction (sample size: 4,349)

The higher the occupational rank of practitioners, the lower was their job change intention. The lowest job change intention proportion was found among high-level personnel (see Figure 4-30).

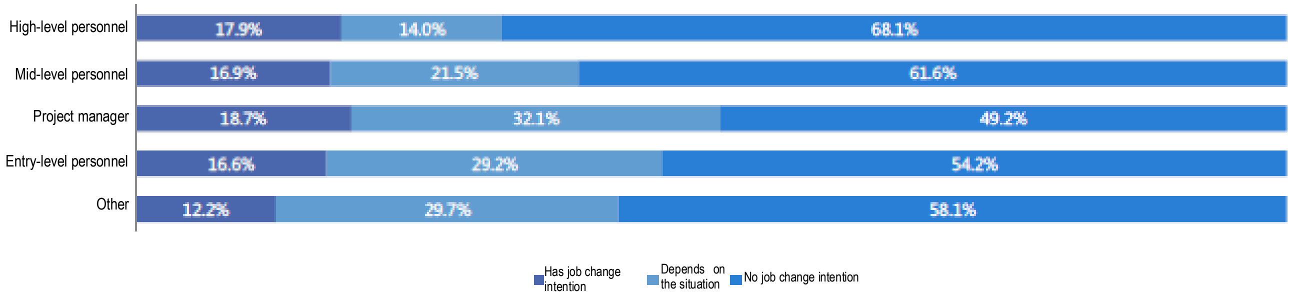


Figure 4-30 Respondent job change intentions, by work position (sample size: 4,349)

4. Job-seeking channels for information security professionals have become more diverse

The sample data shows that more than half of information security professionals tended to search for employers through recruitment websites (53.2%). The next most common approaches were recommendations of industry professionals (46.7%) and recommendations of friends (42.2%) (see Figure 4-31). However, relative to the previous year's 64.5%, the proportion of the sample population that searched for work via recruitment websites dropped 11.3 percentage points. In contrast, there were varying degrees of growth in the proportion of practitioners who searched for employers through head-hunting companies, talent job fairs, industry conference events, and in other ways. Job-seeking channels became more diverse for information security professionals, indicating that China's information security industry talent recruitment market has been gradually developing and improving. Job-seeking channels for information security professionals have become more diverse

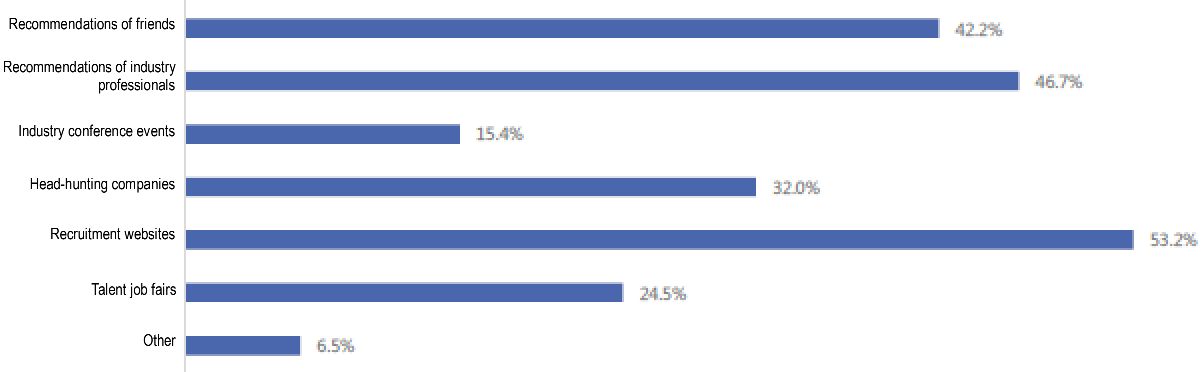


Figure 4-31 Information security practitioner job-seeking channels (sample size: 4,349)

Analysis of the job-seeking channels used by information security professionals of different work positions revealed that entry-level practitioners mainly sought employment through recruitment websites (64.0%); project managers mainly sought employment through the recommendations of industry professionals and recruitment websites (57.5% and 52.0%, respectively); high-level and mid-level practitioners mainly sought employment through the recommendations of industry professionals and head-hunting companies (high-level: 43.4% and 35.5%; mid-level: 49.1% and 41.2%). There was an obvious rise in the proportions of high-level and mid-level practitioners seeking employment through head-hunting companies relative to the previous year (16.1 percentage points and 21.5 percentage points, respectively.) This clearly indicates that high-level and mid-level information security talent have become prizes that various enterprises and public institutions compete among themselves to win (see Figure 4-32).

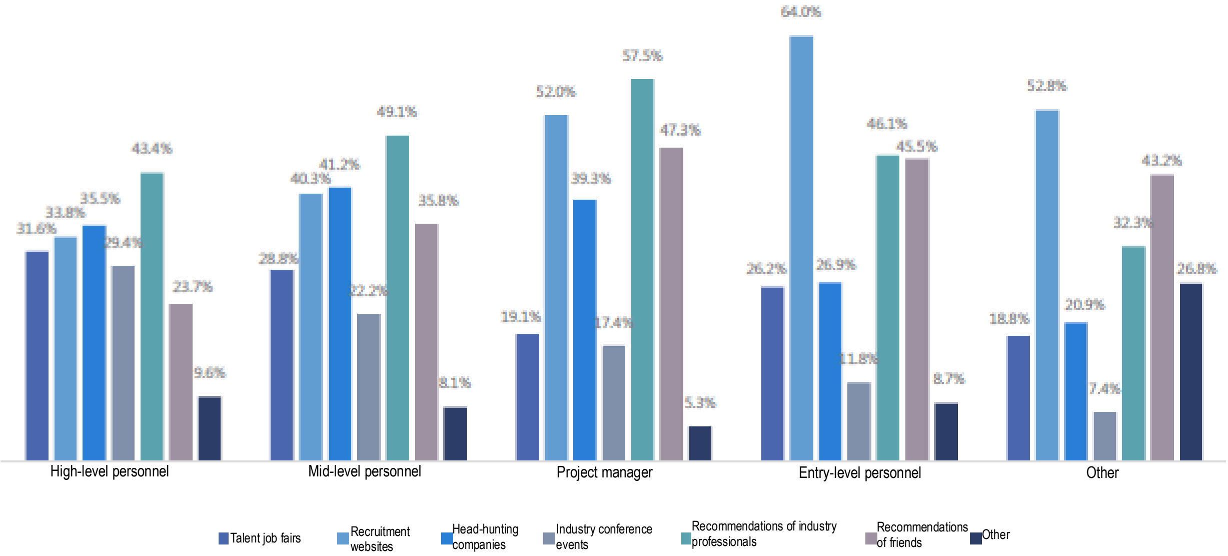


Figure 4-32 Respondent job-seeking channels, by work position (sample size: 4,349)

5. Employers attached greater importance to credentials and relevant work experience

The study found that the majority of employers expected that information security professionals would have relatively strong practical ability and would be able to fit into the work environment relatively quickly. "Information security credentials" capable of demonstrating that the job applicant had a certain amount of professional knowledge, skill, and work experience replaced the previous year's "relevant work experience" as the primary focus of employers. Information security credentials have become an important indicator for employer talent selection. In addition, as cyberspace security became increasingly solidly established as an academic discipline, employers placed more value on advanced educational backgrounds (5.2 percentage point rise over the previous year) (see Figure 4-33).

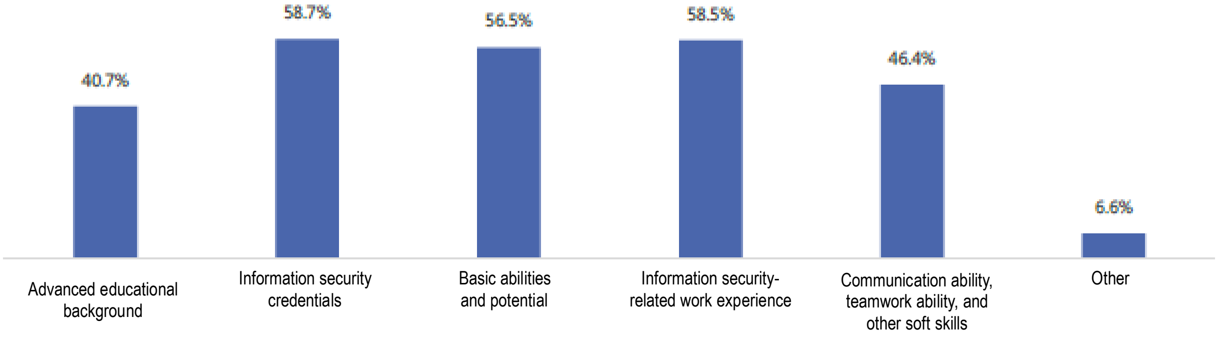


Figure 4-33 Information security practitioner personal qualifications valued by employers (sample size: 4,349)

From the perspective of work unit nature, we find that, with the exception of other non-categorized work units, more than half of respondents believed that the possession of an information security professional credential was what employers valued most in talent. Regard for information security professional credentials was highest among respondents at SOEs, scientific research institutes, Party and government agencies and public institutions, enterprises with foreign company investment, and enterprises with Hong Kong, Macau, and Taiwan investment. The majority of private enterprise respondents believed that employers had relatively high demand for information security-related work experience (65.9%) among talent. The next highest demands were for basic abilities and development potential (59.7%) and the possession of an information security professional credential (58.6%) (see Figure 4-34).

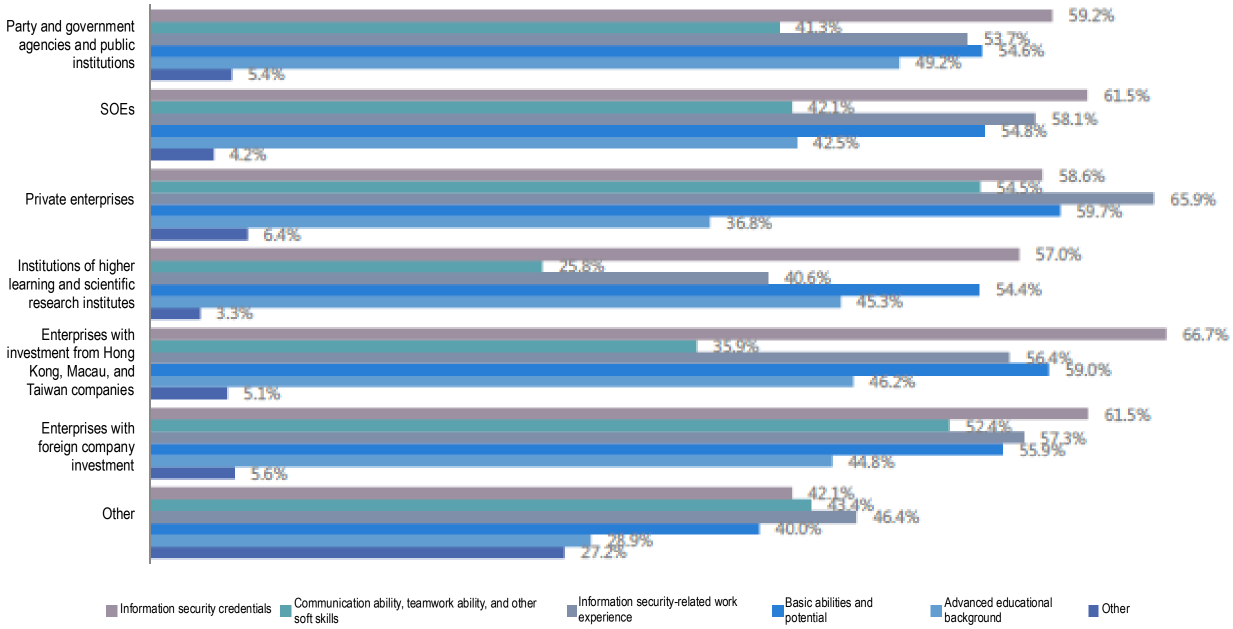


Figure 4-34 Talent qualifications valued by employers, by work unit nature (sample size: 4,349)

5. Ability Enhancement

Talent is the number-one resource. The core of strategic human resources management lies in viewing people as important assets and, through inputs such as education and training, continuously improving their knowledge, skills, and personal qualities so that they can better achieve the business goals of employers. In a field such as information security, where technologies are rapidly developed and replaced, there is an even more pressing need for practitioners to update their knowledge and enhance their professional abilities. The ability of employers to provide sufficient training, continuously improve the professional skills of talent, and help them to achieve self-realization of values will play an increasingly important role in the work of talent recruitment and talent retention.

The *Cybersecurity Law* stipulates that: “The state shall provide support to enterprises, institutions of higher learning, vocational schools, and other educational and training institutions to conduct cybersecurity-related education and training and adopt multiple approaches to cultivate cybersecurity talent”; and that operators of critical information infrastructure shall “periodically provide practitioners with cybersecurity education, technical training and skills assessment.” Cybersecurity is an interdisciplinary subject that covers fields such as computer science, electronics, communications, mathematics, law, and management. It is also an emerging subject that is undergoing continuous updating as information technology develops. The new generation of network information technology as represented by cloud computing, big data, artificial intelligence (AI), the Internet of Things (IoT), and the mobile internet is becoming fused with all economic and social fields at an accelerating rate. These new technological development trends have expanded the meaning of information security and have imposed new requirements on information security professionals. The focus of this chapter is mainly on three areas of the study: Demand for practitioner ability enhancement, training provided by employers, and professional information security credentials.

The Demand for Practitioner Ability Enhancement

Information security professionals need to quickly learn and master relevant skills and knowledge in order to keep up with the updating of information security-related technologies and knowledge. In this study, “occupational training,” having the advantages of frequent updating and being highly focused and tightly bound to the industry’s cutting edge, replaced “self-taught learning” of the previous year as the favorite form of ability enhancement among information security professionals (68.8%). There was a demand among practitioners for ability enhancement in each narrowly defined orientation of professional knowledge and ability. The directions in which they most wished to pursue enhancement were closely tied to information technology development hot spots. Ranked in order of strongest to weakest, they were: Big data security (49.0%), cloud security (41.1%), security management (41.1%) and penetration testing (37.1%).

Training Provided by Employers

Employer internal information security staff training systems have been poorly implemented. 74.9% of work units where information security professionals are employed established information security staff training systems, but only 23.1% of respondents believed the training systems at the units obtained good training results. At the same time, there has not been much willingness or effort on the part of employers to financially aid practitioners so that they can receive occupational training. Only 18.5% provided financial aid at 50% or more. 33.5% of practitioners stated that their own work units did not provide any financial aid.

Professional Information Security Credentials

Information security professional credentials are proof that the person has a certain amount of knowledge, ability, and work experience. Determination of credentials is an effective way of evaluating the professional abilities of information security professionals. More than sixty percent (64.7%) of respondents had information security credentials of one type or another. Those holding a Certified Information Security Professional (CISP) credential accounted for the highest proportion (71.8%) of all those with credentials. 83.7% of practitioners expected to obtain an information security credential within the next year, and those among them who hoped to acquire a CISP credential accounted for the highest proportion (68.9%).

Cybersecurity Law of the People's Republic of China

Article 20 The state shall provide support to enterprises, institutions of higher learning, vocational schools, and other educational and training institutions to conduct cybersecurity-related education and training, adopt multiple approaches to cultivate cybersecurity talent, and promote exchanges among cybersecurity talent.

Article 34(2) (Operators of critical information infrastructure shall) periodically provide practitioners with cybersecurity education, technical training, and skills assessment.

I. The Demand for Practitioner Ability Enhancement

1. Occupational training has become the preferred form of ability enhancement

The study shows that "occupational training," having the advantages of frequent updating and being highly focused and tightly bound to the industry's cutting edge, replaced "self-taught learning" of the previous year as the favorite form of ability enhancement among information security professionals (68.8%). After "occupational training," the choices were, in order of preference: Self-taught learning (44.1%), in-work unit training (41.5%), and industry conferences and workshops (41.2%). Those who expected to enhance their own abilities through degree-granting education accounted for the lowest proportion (31.6%) (see Figure 5-1).

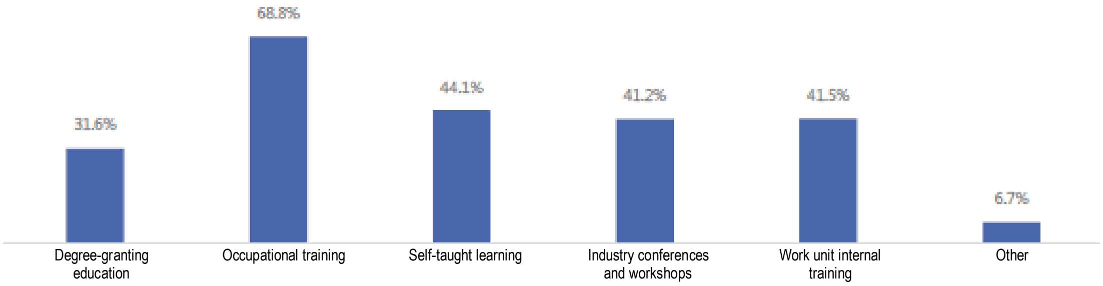


Figure 5-1 Form of ability enhancement expected by respondent (sample size: 4,349)

Respondents in different work positions had varying views on forms of ability enhancement. 72.7% of high-level respondents expected to enhance their abilities through occupational training. Respondents in high-level work positions held degree-granting education in relatively high regard, with 38.9% of high-level respondents hoping to enhance their own abilities through degree-granting education. This is higher than the average percentage of 31.6%. Entry-level respondents tended to choose "self-taught learning." 50.5% of entry-level practitioners chose to enhance their abilities through self-taught learning, while 39.3% of those in high-level positions chose "self-taught learning" (see Figure 5-2).

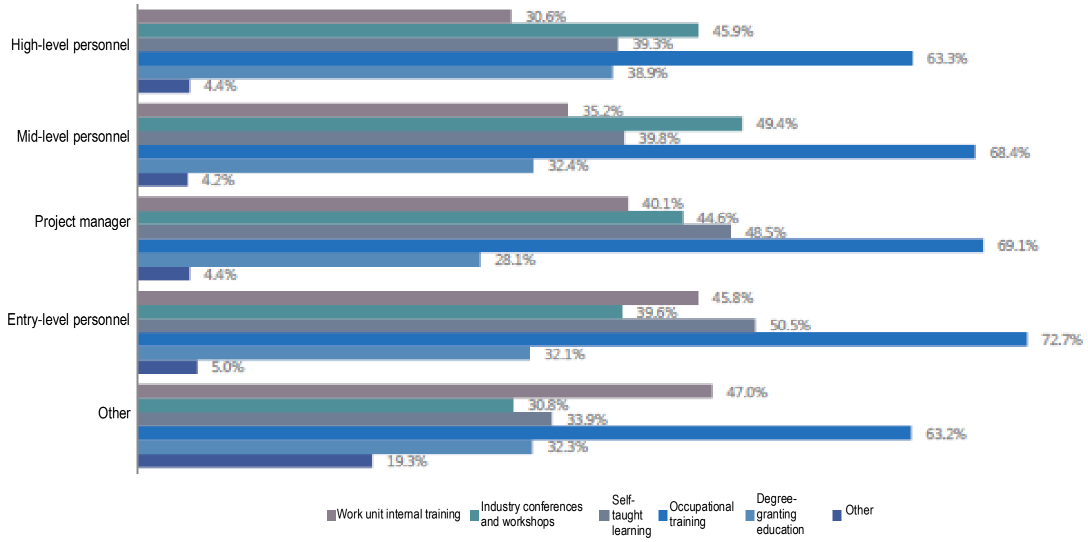


Figure 5-2 Form of ability enhancement expected by respondent, by work position (sample size: 4,349)

2. The demand for ability enhancement covered each narrowly defined professional orientation

The study data shows that there was a demand among practitioners for ability enhancement in each narrowly defined orientation of professional knowledge and skill. The directions in which they most wished to pursue enhancement were closely tied to information technology development hot spots. Ranked in order of strongest to weakest, they were: Big data security (49.0%), cloud security (41.1%), security management (41.1%) and penetration testing (37.1%) (see Figure 5-3).

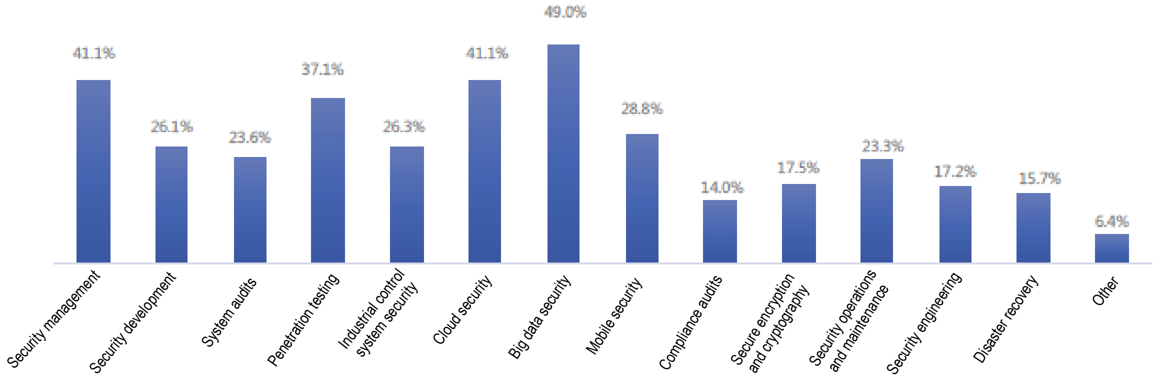


Figure 5-3 Professional abilities practitioners hope to enhance (sample size: 4,349)

II. Training Provided by Employers

1. The majority of practitioners were dissatisfied with the results of internal training in their units

According to the study data, 74.9% of work units where information security professionals were employed established information security staff training systems, but only 23.1% of respondents believed the training systems at the units obtained good training results. 51.8% of practitioners evaluated their unit's internal information security training results as "average" or "still no obvious results" (see Figure 5-4).

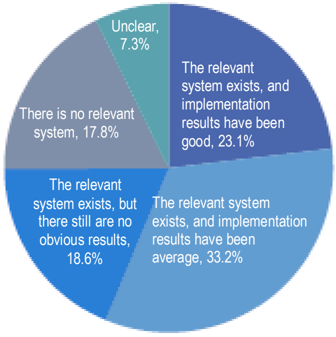


Figure 5-4 Information security practitioner training system setup and implementation (sample size: 4,349)

In scientific research institutions and institutions of higher learning, government agencies and public institutions, and the information technology, telecommunications, and internet industry, the establishment of training systems and the implementation results of training were slightly better than in other industries (see Figure 5-5).

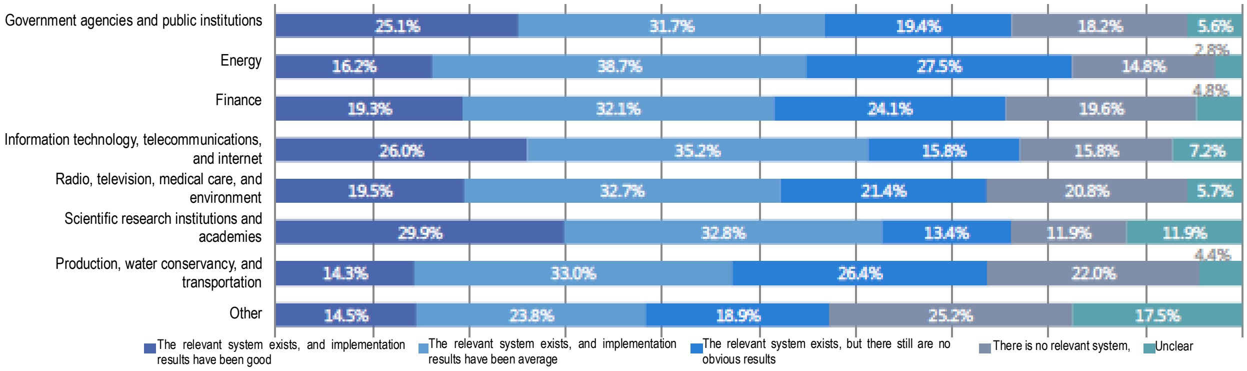


Figure 5-5 Internal training system setup and implementation, by industry (sample size: 4,349)

From the perspective of work unit nature, we find that respondents in SOEs were less likely than in other industries to regard internal training as having "good implementation results" while being more likely to regard it as having "average implementation results" than in other industries (see Figure 5-6).

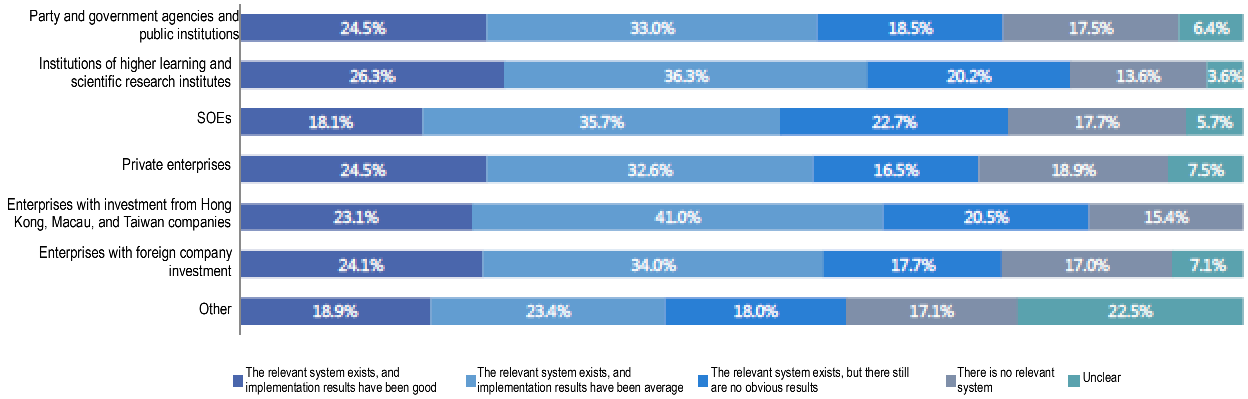


Figure 5-6 Internal training system setup and implementation, by work unit nature (sample size: 4,349)

2. Unit Financial Support Failed to Meet Demand for Practitioner Ability Enhancement

66.5% of information security professionals stated that their work units financially supported employee participation in information security occupational training, but that the financial support was relatively weak. The majority of units provided occupational training financial support in an amount less than 25%, and only 18.5% provided professionals with financial support at above 50%. 33.5% of professionals stated that their current work units did not provide any financial aid (see Figure 5-7).

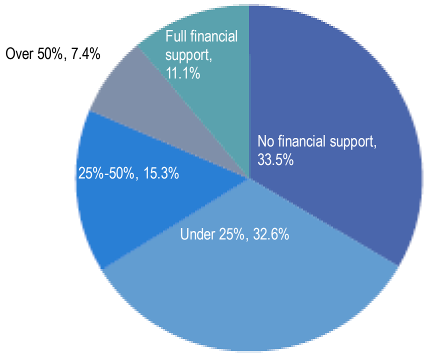


Figure 5-7 Amount of occupational training financial support provided by work units for employees (sample size: 4,349)

From the perspective of industry, we find that energy, finance, production, water conservancy and transportation, and scientific research institutions and institutes provided relatively high proportions of financial support for employee occupational training (see Figure 5-8).

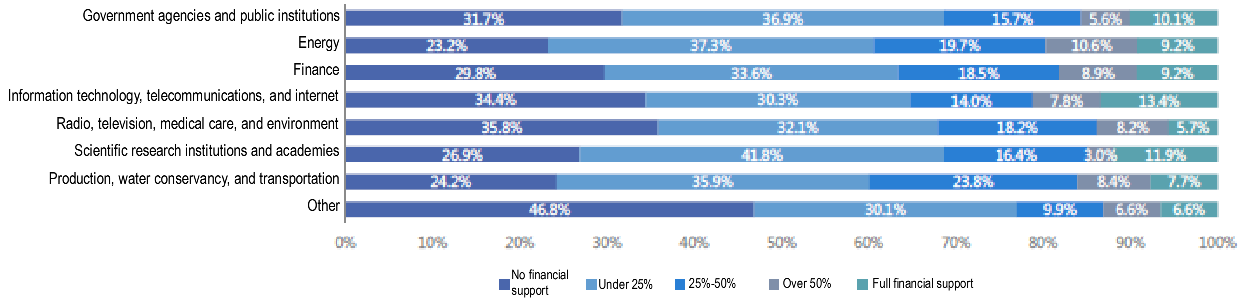


Figure 5-8 Amount of occupational training financial support provided by work units for employees, by industry

(sample size: 4,349)

From the perspective of work unit nature, we find that SOEs and institutions of higher learning and scientific research institutes provided relatively high proportions of financial support for employee occupational training (see Figure 5-9).

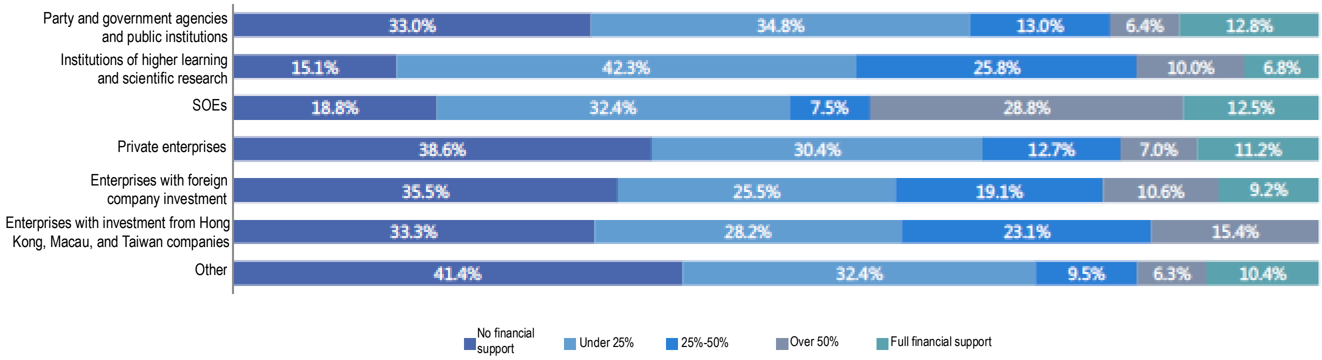


Figure 5-9 Amount of occupational training financial support provided by work units for employees, by work unit nature (sample size: 4,349)

III. The Situation Concerning Professional Information Security Credentials

1. CISP credentials were held or sought after by the largest number of practitioners

The study shows that more than sixty percent (64.7%) of respondents had information security credentials of one type or another. The proportion of credentialed practitioners increased 9.2 percentage points (see Figure 5-10).

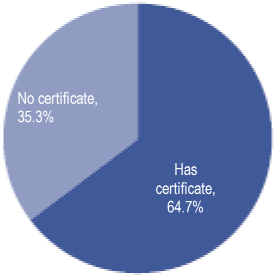


Figure 5-10 Respondent credential status (sample size: 4,349)

According to the data, the higher the work position, the higher the proportion of credentialed professionals. 84.3% of high-level respondents held information security credentials of one type or another. The percentage for entry-level respondents was 57.8%, which was lower than average (64.7%) (see Figure 5-11).

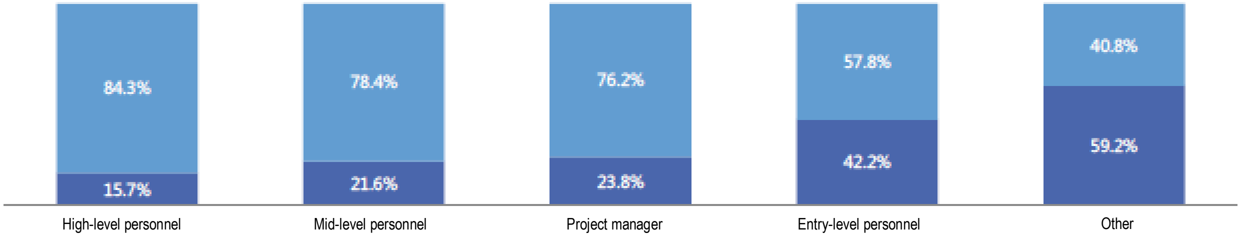


Figure 5-11 Respondent credential possession, by work position (sample size: 4,349)

Respondent evaluations of the credential-holding status of information security professionals in their current work units were not optimistic. Only 30.1% believed that authoritative cybersecurity credentials recognized within the industry were "held by relatively many" or "generally held" (see Figure 5-12).

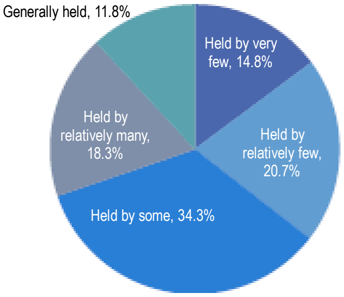


Figure 5-12 Evaluation of credential status (sample size: 4,349)

Those holding a Certified Information Security Professional (CISP) credential accounted for the highest proportion (71.8%) of all those with credentials (see Figure 5-13).

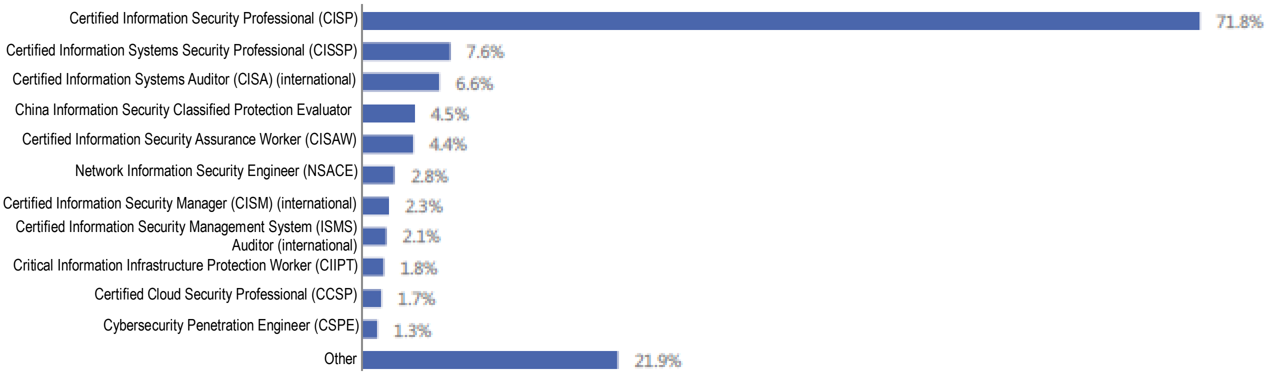


Figure 5-13 Types of information security credentials held by respondents (sample size: 2,819)

The Certified Information Security Engineer credential (CISE) was held by the largest number of CISP holders, accounting for 44.1% of the total (see Figure 5-14).

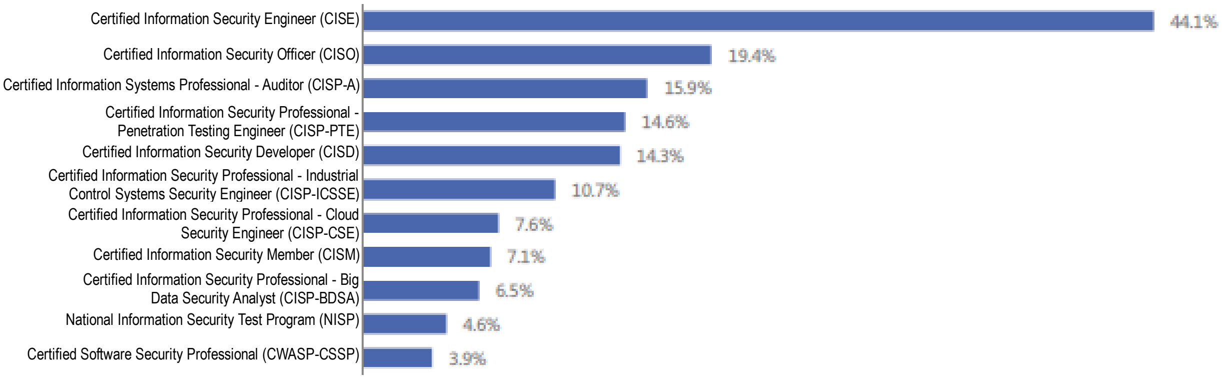


Figure 5-14 Information on Certified Information Security Professional (CISP) credentials held (sample size: 2,024)

83.7% of practitioners expected to obtain an information security credential within the next year, and those among them who hoped to acquire a Certified Information Security Professional (CISP) credential accounted for the highest proportion (68.9%) (see Figure 5-15).

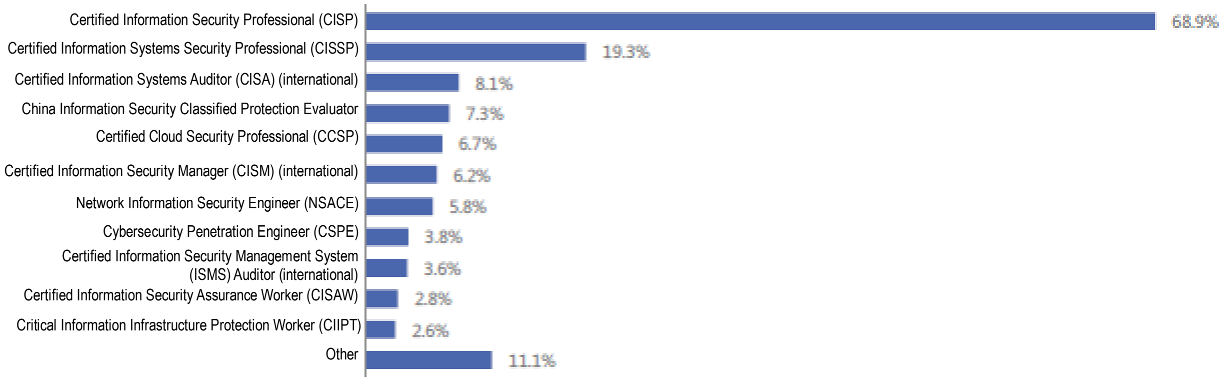


Figure 5-15 Credentials which respondents hope to acquire during the next year (sample size: 3,573)

2. Practitioners that held credentials had higher annual salaries and salary increases than those who did not

The data shows that the mean annual salary of practitioners holding information security credentials was approximately RMB 169,000, which was higher than the mean annual salary of RMB 135,000 of those who do not hold credentials (see Figure 5-16).

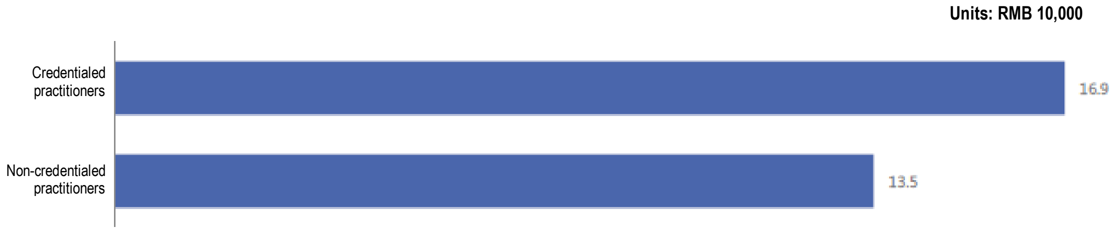


Figure 5-16 Effect of information security credentials on salary (sample size: 4,347)

During the past year, more than sixty percent of credentialed practitioners saw their salaries rise to one degree or another. In contrast, the salaries of more than half of non-credentialed practitioners either did not increase or in fact decreased (see Figure 5-17).

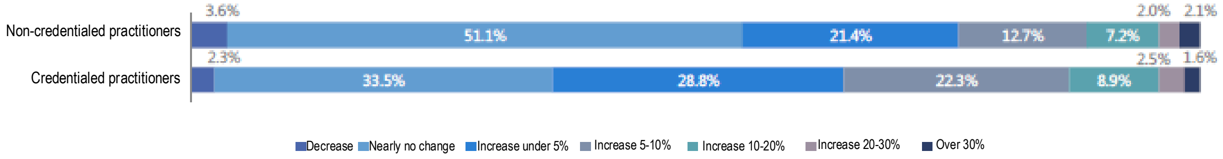


Figure 5-17 Effect of credential-holding status on past-year salary increases (sample size: 4,349)

64.2% of credentialed practitioners saw their salaries rise, an increase of 2.8 percentage points over the previous year (61.4%). The proportion of practitioners holding Certified Information Security Professional (CISP) credentials who saw their annual salaries rise in the past year (70.8%) was 6.2 percentage points higher than for other credential holders (64.6%) (see Figure 5-18).

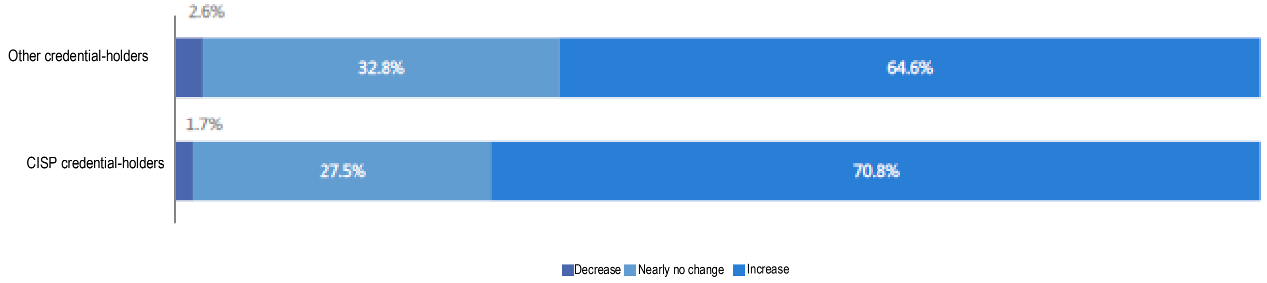


Figure 5-18 Effect of different security credentials on prior-year salary (sample size: 2,819)

3. CISP certificates provided a greater boost to the career development of information security professionals

Relative to other credential-holders, practitioners who held Certified Information Security Professional (CISP) certificates believed that information security professional credentials gave a bigger boost to their career development (63.7%), an increase of 1.6 percentage points over the previous year's 62.1% (see Figure 5-19).

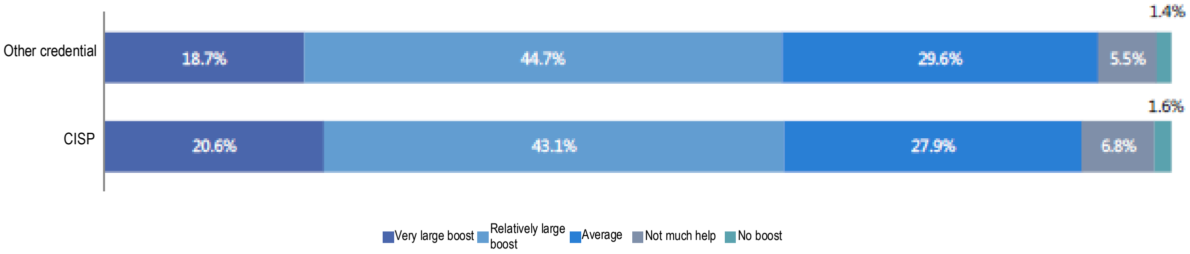


Figure 5-19 Degree of practitioner career boost, by security credential (sample size: 2,819)

4. CISP subcategories followed demand for practitioner ability enhancement

The CISP credentials that practitioners most hoped to acquire within the coming year were: Certified Information Security Engineer (CISE), Certified Information Security Professional - Penetration Testing Engineer (CISP-PTE), Certified Information Systems Professional - Auditor (CISP-A), Certified Information Security Professional - Cloud Security Engineer (CISP-CSE), and Certified Information Security Officer (CISO) (see Figure 5-10), which basically covered the professional ability orientations (e.g., big data security, cloud security, security management, and penetration testing) that Chinese information security professionals most hoped to enhance (see 6-21). Thus, they follow the actual professional ability enhancement demand of professionals.

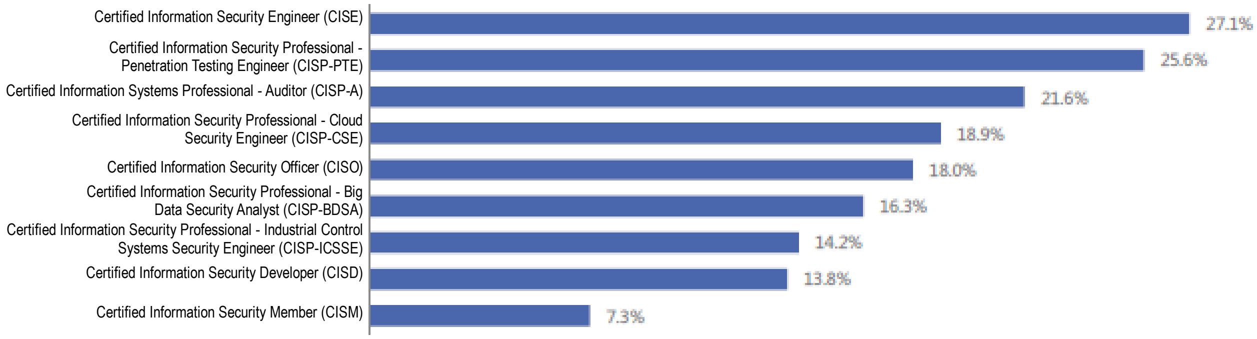


Figure 5-20 Certified Information Security Professional (CISP) credentials which respondents expect to acquire in the coming year (sample size: 2,461)

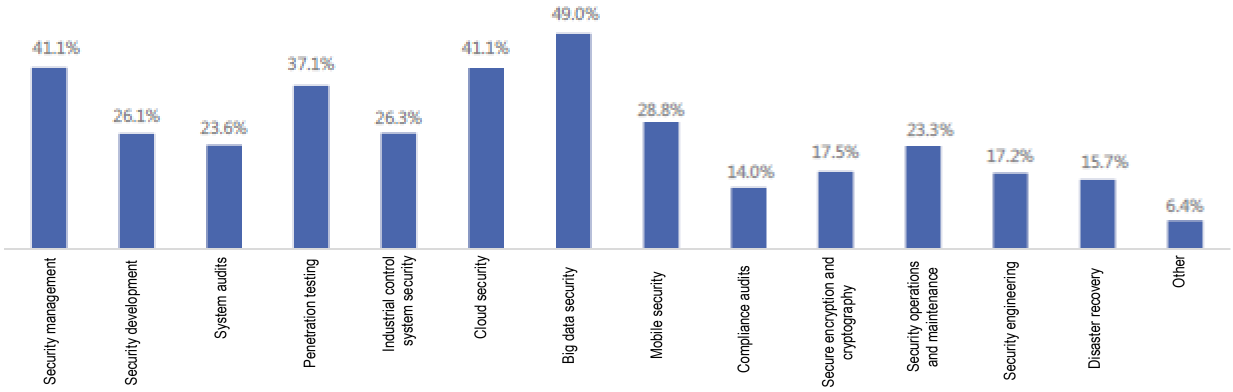


Figure 5-21 Professional abilities practitioners hope to enhance (sample size: 4,349)

6. Institutional Environment

Organizational safeguards are an important precondition for launching cybersecurity work. Having specialized personnel in specialized positions performing specialized work helps to implement cybersecurity work responsibilities. China's *Cybersecurity Law* clearly stipulates that network operators shall "determine the persons in charge of cybersecurity and determine cybersecurity protection responsibilities" and that "critical information infrastructure operators shall set up specialized security management bodies and assign persons in charge of security management. Moreover, they shall perform security background checks on such persons and on other personnel filling critical positions." In addition, the state encourages network operators of non-critical information infrastructure to voluntarily participate in critical information infrastructure protection systems.

A complete cybersecurity talent development policy should, in addition to including talent education and training (for the relevant study content, see *Chapter 5: Ability Enhancement*), also include a talent appraisal and discovery system, a motivation assurance system, and a talent security system. This chapter studies the following among government and business units mainly from the four perspectives of responsible entities, motivation assurance, talent appraisal, and talent security: Implementation of cybersecurity management departments and persons in charge, establishment of career advancement channels and work incentive mechanisms, evaluation of information security practitioner professional ability, and personnel security background checks.

I. Responsible Entities

II. Motivation Assurance

III. Talent Appraisal

IV. Talent Security

Responsible Entities

The study results show that nearly seventy percent of work units where information security professionals were employed had set up specialized cybersecurity management departments and assigned persons to be in charge of cybersecurity management. The establishment of specialized cybersecurity management departments and person-in-charge mechanisms can effectively improve the phenomenon of part-time practitioners. However, 57.7% of the practitioners in units that had already established mechanisms were also responsible for other non-security work. Information security departments and person-in-charge systems set up by critical information infrastructure operators generally have been in practice for several years. After the *Cybersecurity Law* went into effect, a greater effort was made to upgrade security departments, add to the number of security positions, improve the professionalism of security teams, and so on. However, the phenomenon of "personnel-post mismatch" is now quite widespread. In some cases, practitioners do not have the ability required by the position. In other cases, the job title is that of a specialized information security position, but the work actually done by the person filling the position is informatization or some other such work.

Motivation Assurance

The study shows that 65.5% of information security professionals stated that the personnel management department of their work unit established career advancement channels and work incentive mechanisms for information security professionals, but less than twenty percent believed that the relevant mechanisms had "good implementation results." In units that had established information security personnel career advancement channels and work incentive mechanisms, practitioner mean annual salary and occupational satisfaction levels were higher than in units without such mechanisms.

Talent Appraisal

The distribution of information security practitioner positions in China was basically the same as in the previous year. Entry-level information security engineers accounted for 38.0%. The data from this job title survey shows that information security professionals having a mid-level position title accounted for the greatest number, being roughly 30.5% of the total. Among respondents whose job titles could be clearly categorized, the majority of position titles fell within the engineering and technology category (81.7%). At the same time, 43.7% of information security professionals believed that their job title could not be clearly categorized, an obvious increase over the previous year's figure (25.9%).

Talent Security

As the social credit system is gradually perfected and commercial background checking services develop, "new employee background checks" are becoming increasingly common. The study shows that 63% of practitioners needed to undergo some form of background check prior to employment. The background check work of employers such as Party and government agencies and public institutions, institutions of higher learning and scientific research institutes, and SOEs is usually the responsibility of the personnel department. Enterprises with foreign company investment and enterprises with Hong Kong, Macau, and Taiwan company investment tend to entrust such work to professional third-party organizations.

Cybersecurity Law of the People's Republic of China

Article 21(1) (Network operators shall) establish internal security management policies and operating procedures, determine the persons in charge of cybersecurity, and discharge the responsibilities for cybersecurity protection.

Article 34(1) (Critical information infrastructure operators shall) set up specialized security management bodies and assign persons in charge of security management. Moreover, they shall perform security background checks on such persons and on other personnel filling critical positions.

I. Cybersecurity management departments and person-in-charge mechanisms helped to reduce the part-time phenomenon

Nearly seventy percent of respondents stated that their work units had set up a specialized cybersecurity management department and put someone in charge. Nearly twenty percent of respondents stated that they had not set up a relevant structure or put someone in charge.

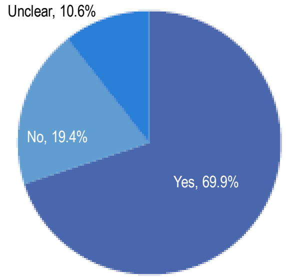


Figure 6-1 Implementation of cybersecurity department with full-time, specialized positions and person in charge (sample size: 4,349)

The study data show that, in units that had established a cybersecurity management department and a person in charge mechanism, 42.3% of practitioners did not need to be responsible for non-security work. This was 13.7 percentage points higher than in units without the relevant system. There was a decline in the part-time practitioner phenomenon, but 57.7% of practitioners still had additional responsibilities related to non-security work (see Figure 6-2).

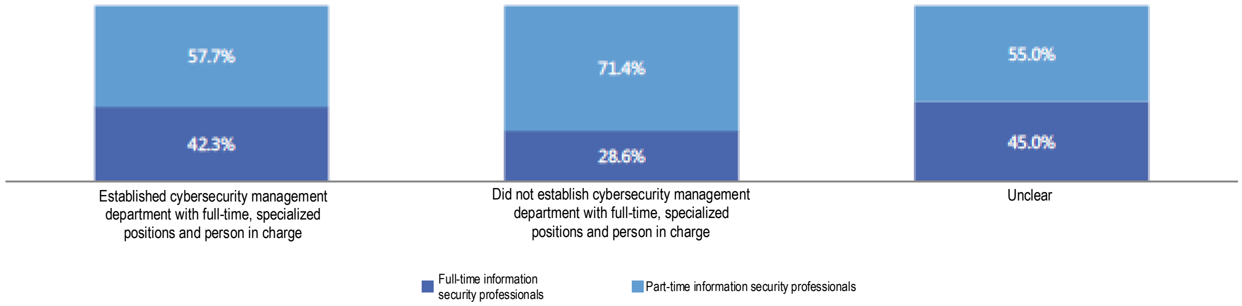


Figure 6-2 Effect of implementing cybersecurity management department having full-time, specialized positions and person in charge on practitioner "part-time" status (sample size: 4,349)

From the perspective of industry, we find that in finance (74.1%), information technology, telecommunications, and internet industry (74.1%), energy (72.5%), and government agencies and public institutions (70.1%) a higher proportion set up cybersecurity management departments and persons in charge (see Figure 6-3).

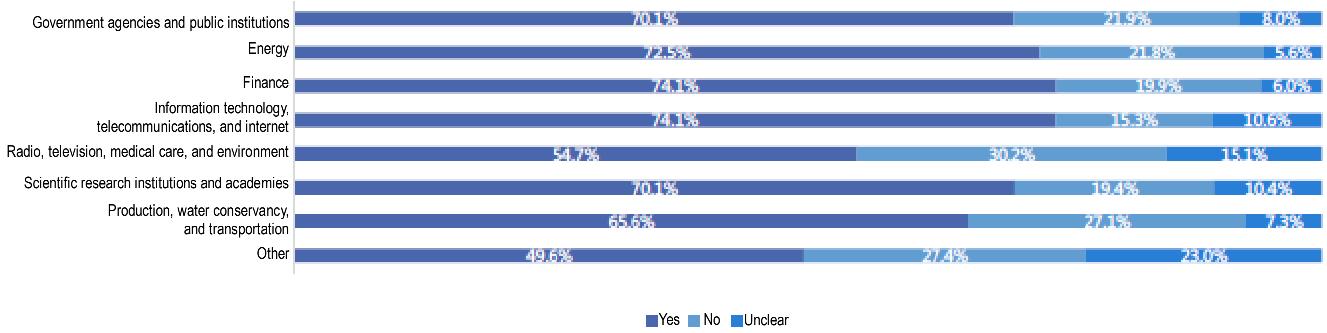


Figure 6-3 Implementation of cybersecurity department with full-time, specialized positions and person in charge, by employer industry (sample size: 4,349)

From the perspective of work unit nature, we find that institutions of higher learning and scientific research institutes (75.2%), enterprises with Hong Kong, Macau, and Taiwan company investment (74.4%), and SOEs are more likely to have set up cybersecurity management departments and persons in charge (see Figure 6-4).

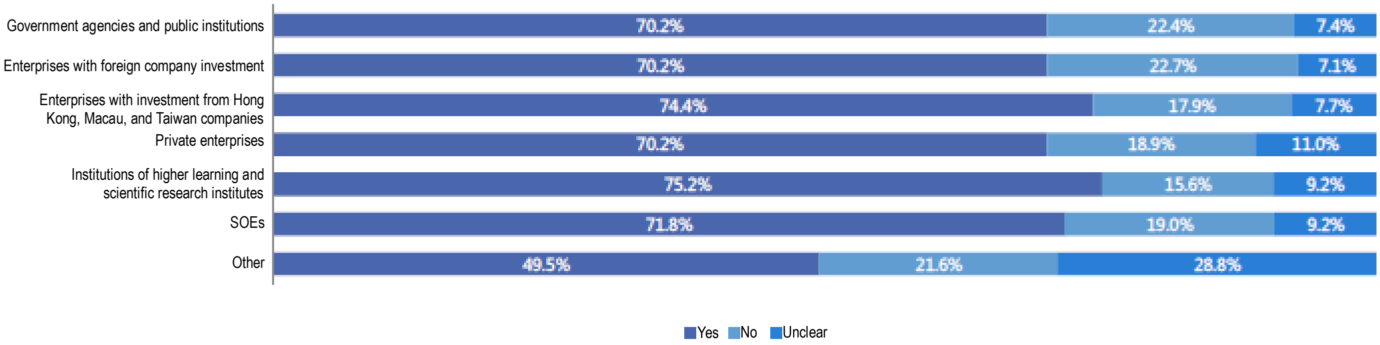


Figure 6-4 Implementation of cybersecurity department with full-time, specialized positions and person in charge, by nature of employer (sample size: 4,349)

From the perspective of number of employees, we find that the more employees an employer has, the more likely that it has set up a cybersecurity management department with full-time, specialized positions and a person-in-charge mechanism. 76.2% of employers with more than 1,000 employees had set up cybersecurity management departments with full-time, specialized positions and person-in-charge mechanisms. That is 28 percentage points higher than for employers having fewer than 20 employees (see Figure 6-5).

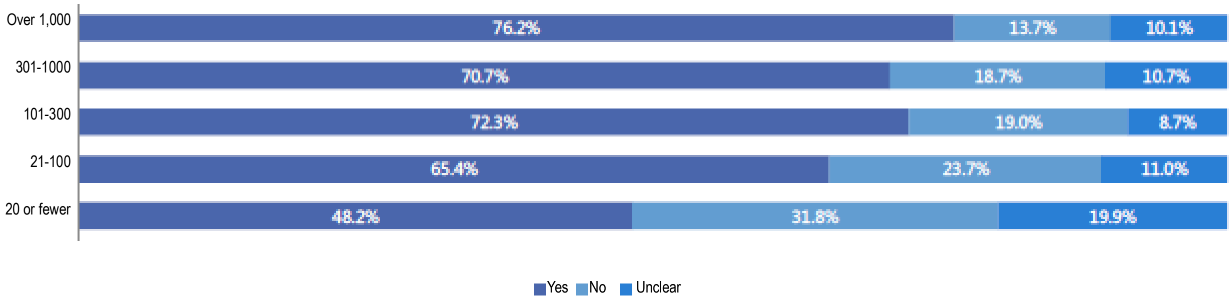


Figure 6-5 Implementation of cybersecurity management departments and persons in charge, by number of organization employees (sample size: 4,349)

II. The effects of existing career advancement channels and incentive mechanisms were not yet obvious

The study shows that 65.5% of information security professionals stated that the personnel management department of their work unit had established career advancement channels and work incentive mechanisms for information security professionals, but less than twenty percent believed that the relevant mechanisms had "good implementation results." 46.3% of information security professionals stated that they had reservations about the actual effects of career advancement and work incentive mechanisms (see Figure 6-6).

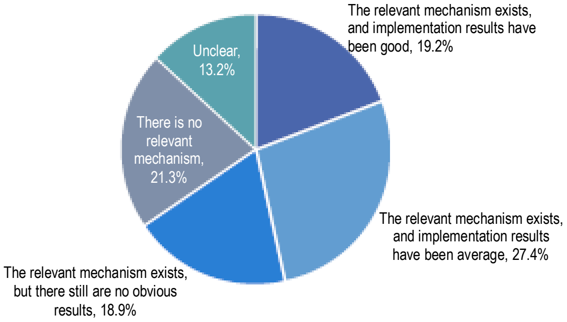


Figure 6-6 Implementation of career advancement channels and incentive mechanisms (sample size: 4,349)

In units that had established information security practitioner career advancement channels and work incentive mechanisms, practitioner mean annual salary and occupational satisfaction levels were higher than in units without such mechanisms. Moreover, the better the relevant mechanisms, the higher the mean annual salary and occupational satisfaction level (see Figures 6-7 and 6-8).

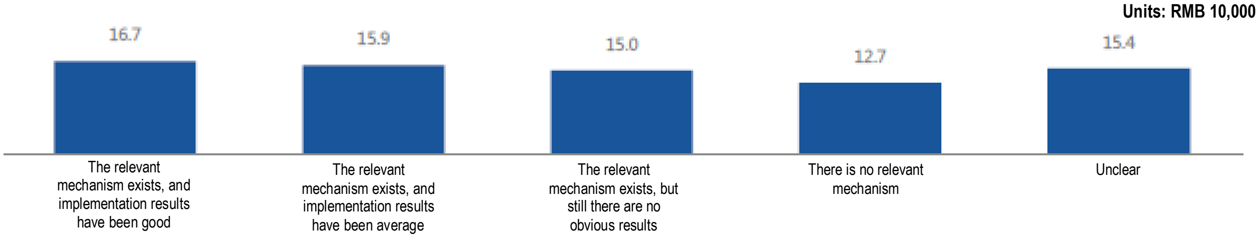


Figure 6-7 Respondent mean annual salary, by implementation results of unit career advancement channels and incentive mechanisms (sample size: 4,347)

In units with good incentive mechanism implementation results, more than sixty percent of practitioners had an occupational satisfaction level that was “rather satisfied “ (47.6%) or “highly satisfied” (13.1%). This was nearly 42 percentage points higher than in units lacking the relevant mechanisms (see Figure 6-8).

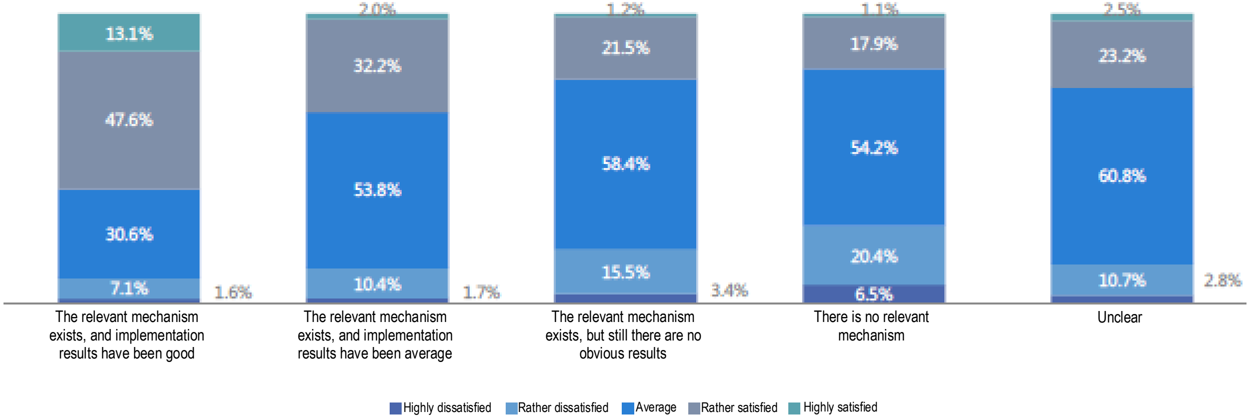


Figure 6-8 Respondent occupational satisfaction level, by implementation results of unit career advancement channels and incentive mechanisms (sample size: 4,349)

III. Mechanisms for appraising information security abilities were in need of improvement

According to the data results of this study, the distribution of information security practitioner positions in China was basically the same as in the previous year. Entry-level information security engineers accounted for the highest proportion, 38.0%. Next were mid-level positions, i.e., security department heads (21.8%) and project managers (19.7%) (see Figure 6-9).

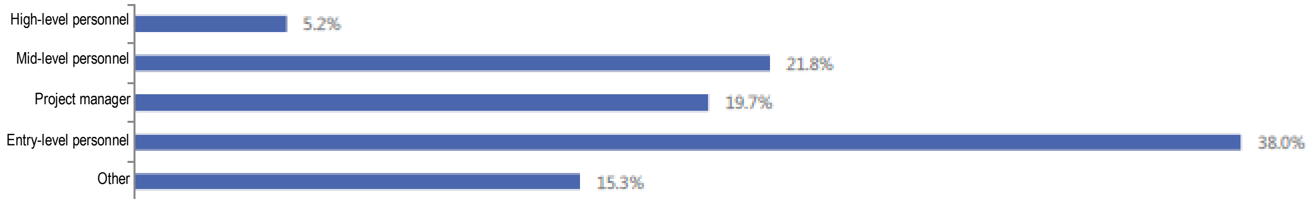


Figure 6-9 Respondent positions (sample size: 4,349)

According to the study sample data, information security professionals having a mid-level job title accounted for the greatest number, being 30.5% of the total. 43.7% of information security professionals believed that their job title could not be clearly categorized (see Figure 6-10), an obvious increase over the previous year’s study data (25.9%).

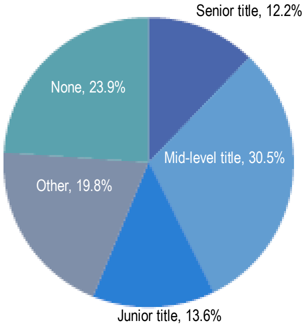


Figure 6-10 Respondent job titles (sample size: 4,349)

Among respondents whose job title could be clearly categorized, the majority of job titles fell within the engineering and technology category (81.7%) (see Figure 6-11).

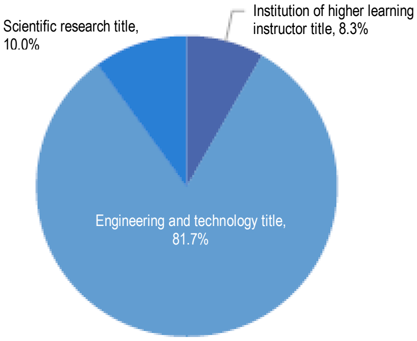


Figure 6-11 Respondent job title categories (sample size: 2,446)

IV. More than sixty percent of practitioners needed to undergo background checks

As the social credit system and commercial background checking services develop, "new employee background checks" are becoming increasingly common. The study shows that 63% of practitioners needed to undergo a background check prior to employment (see Figure 6-12).

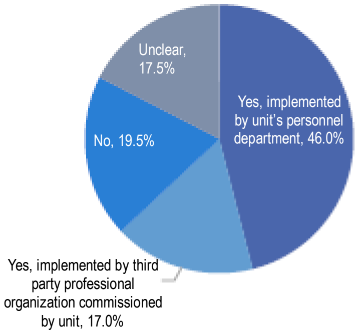


Figure 6-12 Respondent did or did not undergo background check

From the perspective of work unit nature, we find that the background check work of employers such as Party and government agencies and public institutions, institutions of higher learning and scientific research institutes, and SOEs was usually the responsibility of the personnel department. Enterprises with foreign company investment and enterprises with Hong Kong, Macau, and Taiwan company investment tended to entrust such work to professional third-party organizations (see Figure 6-13).

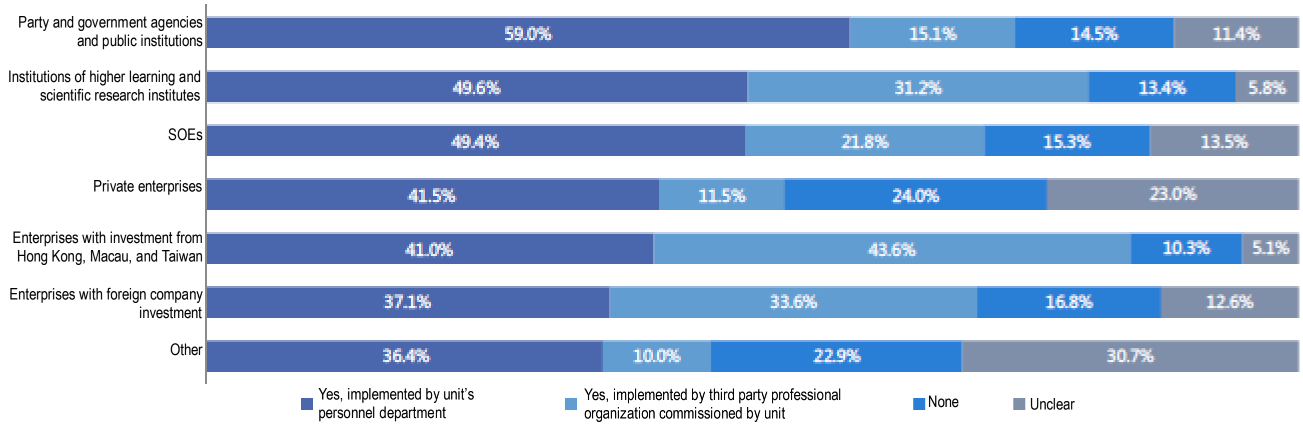


Figure 6-13 Respondent did or did not undergo background check, by work unit nature (sample size: 4,349)

From the perspective of industry, we find that finance (77.4%), scientific research institutions and academies (76.1%), government agencies and public institutions (75.4%), and other such employers were more likely to conduct background checks and tended to make the background check work the responsibility of personnel departments (see Figure 6-14).

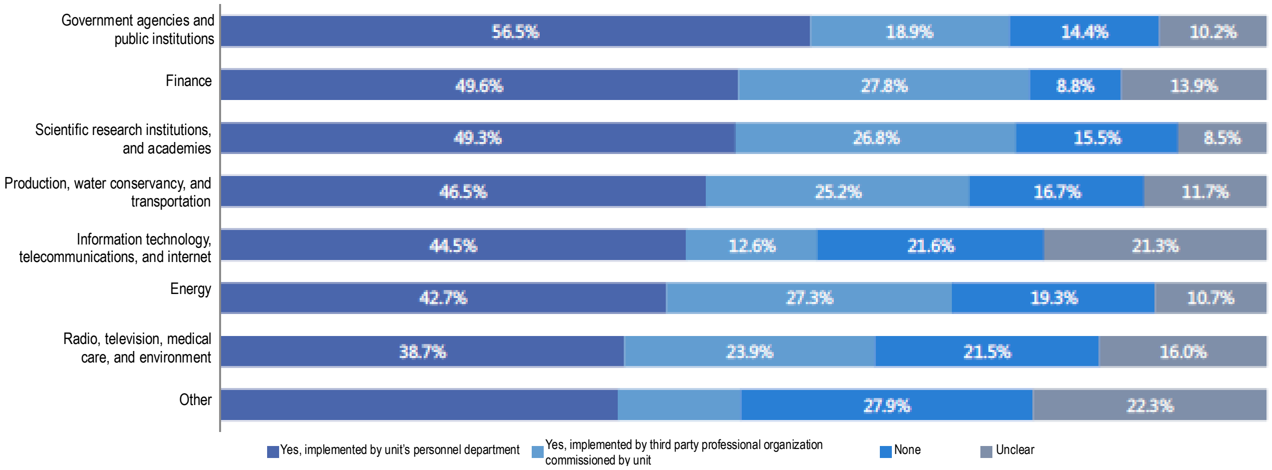


Figure 6-14 Respondent did or did not undergo background check, by industry (sample size: 4,349)

7. Security Situation

Since information security professionals serve as cyber and information security front-line workers and the backbone force in the construction of China as a cyber powerhouse, their views represent the most professional and objective assessments concerning the security situation. This chapter presents current security risks and responses thereto by studying three aspects: Practitioner views of the security situation, security threats faced by units and the security measures they take, and views of security trends.

I. Security Threats

II. Security Measures

III. Security Trends

Impressions of Security Threats

The overall information security situation in China does not permit optimism. The information security threats which practitioners most often confront and handle in their work are, in order of importance: Vulnerability attacks (62%), data leaks (51.2%), and denial-of-service attacks (41.4%), which are consistent with the previous year's study results. Information security incidents continually arise. The main reasons for them are imperfect information security management (58.7%), lack of security training for ordinary employees (58.5%), failure on the part of administrators or senior management to take cybersecurity work seriously (55.4%), and insufficient information security talent and funds (48.7%).

Implementation of Security Measures

The *Cybersecurity Law* clearly stipulates that network operators shall "establish internal security management policies and operating procedures" to discharge the responsibilities for cybersecurity protection. 78% of information security professionals stated that their work units had established internal cybersecurity management policies and operating procedures. However, only one-fourth of practitioners reported that the relevant policies and procedures had had good implementation results (25%). 77.6% of practitioners stated that information security risk evaluation work was already underway in their units. The main ways in which enterprises and public institutions disposed of cybersecurity threats were to resolve them with their own security team (41.8%), and through a combination of internal teams and outsourcing (43.0%).

Perceptions of Security Trends

More than half of information security professionals believed that big data security, cloud computing security, AI security, IoT security, and mobile internet security remain key development directions for the future security industry. Core technologies are pillars of the nation. They "cannot be exchanged on the market or bought with money." As for the core technology that China most needs to achieve domestic production of, "domestic production of chips" replaced the previous year's "domestic production of operating systems" in this study as the option with the highest domestic production priority in the eyes of respondents.

I. Vulnerability attacks and data leaks were still the most common cybersecurity threats

According to security feedback from information security professionals, the information security threats which they most often confronted and handled in their work were, in order of importance: Vulnerability attacks (62%), data leaks (51.2%), and denial-of-service attacks (41.4%), which were consistent with the previous year's study results (see Figure 7-1).

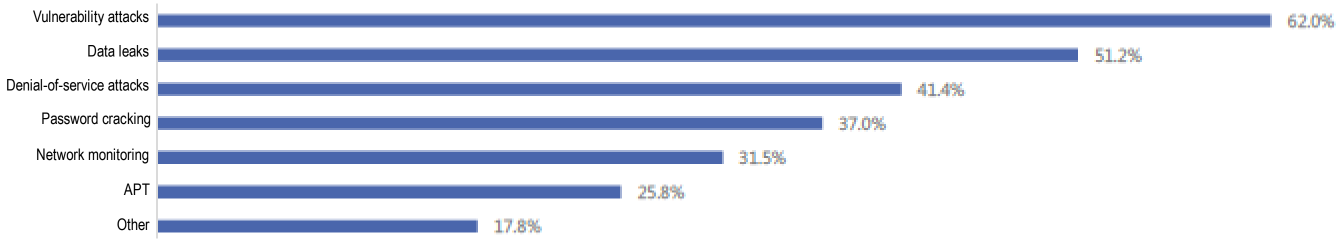


Figure 7-1 Information security threats often confronted and handled by respondents (sample size: 4,349)

The overall distribution of security threats encountered by units in different industries was trending in the same direction. The most prominent threats in each case are vulnerability attacks and data leaks (see Figure 7-2).

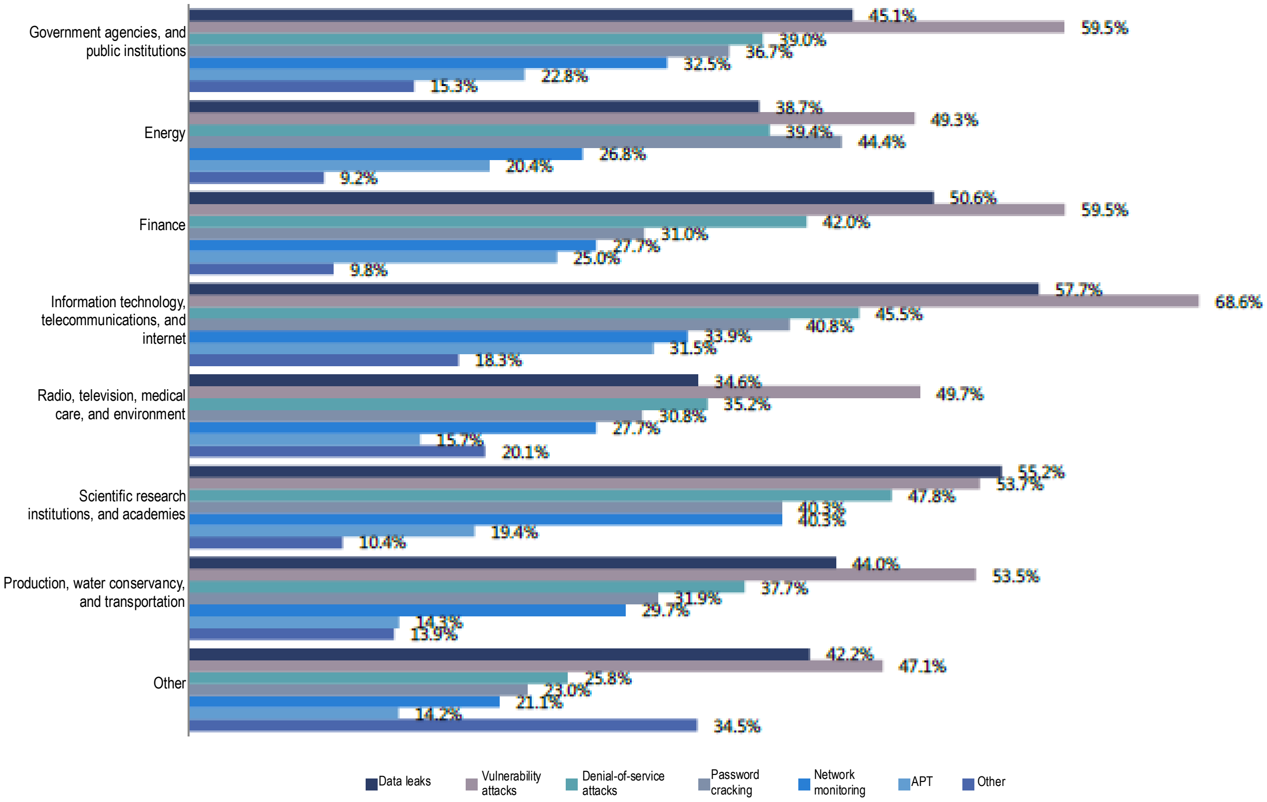


Figure 7-2 Respondent cybersecurity impressions, by industry (sample size: 4,349)

II. The main reasons for security incidents had to do with management, awareness, and insufficient resources

This study included practitioner views on the reasons for information security incidents within the scope of its survey. The study results show that more than half of respondents believed that the main reasons for information security incidents were imperfect information security management (58.7%), lack of security training for ordinary employees (58.5%), failure on the part of administrators or senior management to take information security work seriously (55.4%), and insufficient information security talent and funds (48.7%) (see Figure 7-3).

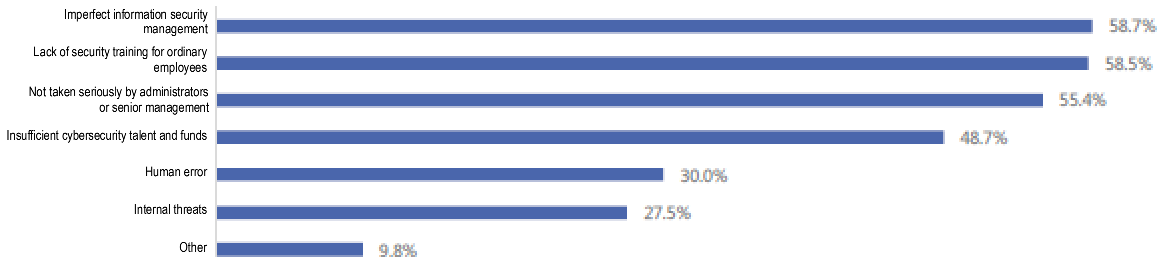


Figure 7-3 Main reasons for information security incidents (sample size: 4,349)

The problem of cybersecurity not being taken seriously by administrators or senior management was particularly pronounced in scientific research institutions and academies, and in radio, television, medical care and the environment. In the finance industry, the problem of lack of security training for ordinary employees was more pronounced. In information technology, telecommunications, and internet industry-related units, more practitioners believed that the main reason was imperfect information security management (see Figure 7-4).

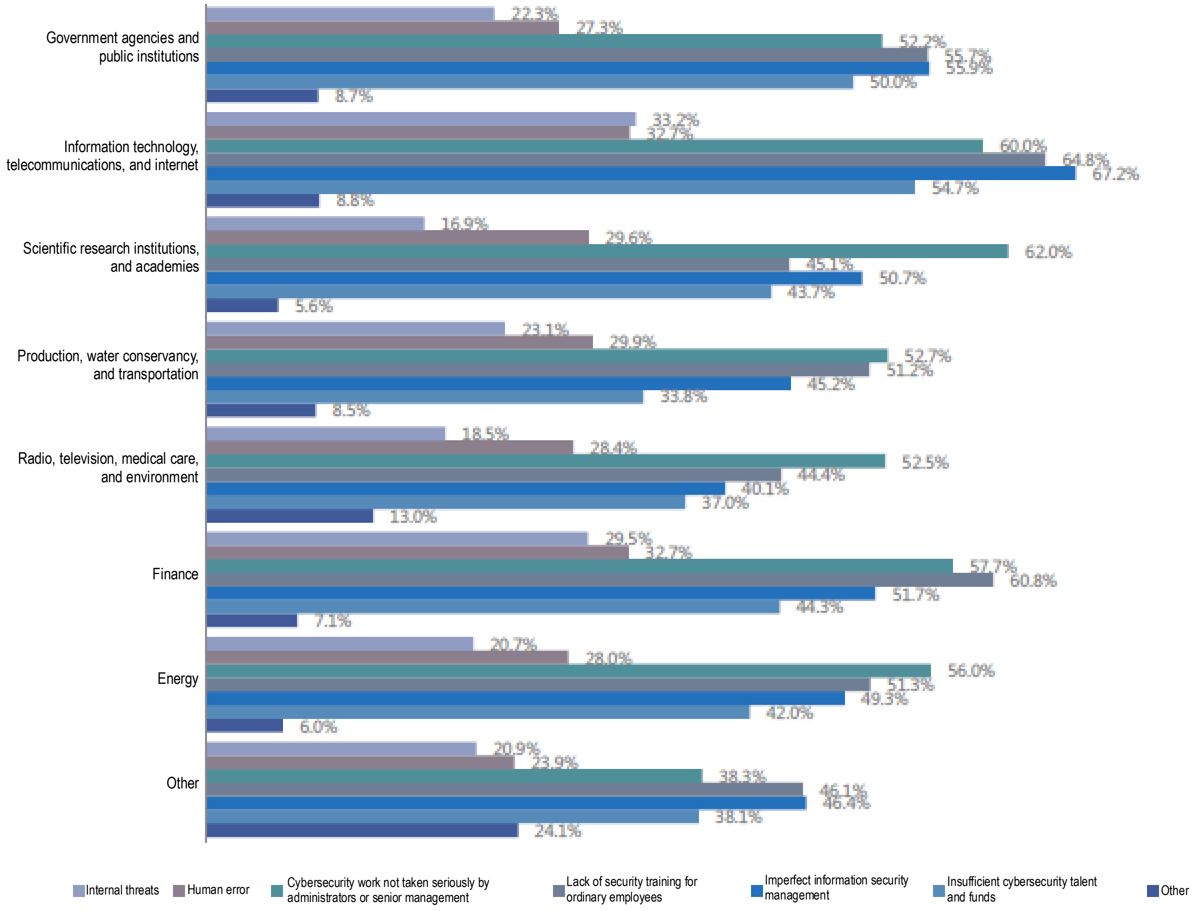


Figure 7-4 Main reasons for information security incidents, by industry (sample size: 4,349)

III. The majority of units established cybersecurity policies and operating procedures

The *Cybersecurity Law* clearly stipulates that network operators shall "establish internal security management policies and operating procedures" to discharge the responsibilities for cybersecurity protection. The study shows that 78% of information security professionals stated that their work units had established internal cybersecurity management policies and operating procedures. However, only one-fourth of practitioners report that the relevant policies and procedures had good implementation results (25%). More than half of practitioners were dissatisfied with the implementation results. Implementation of the relevant policies is in need of improvement (see Figure 7-5).

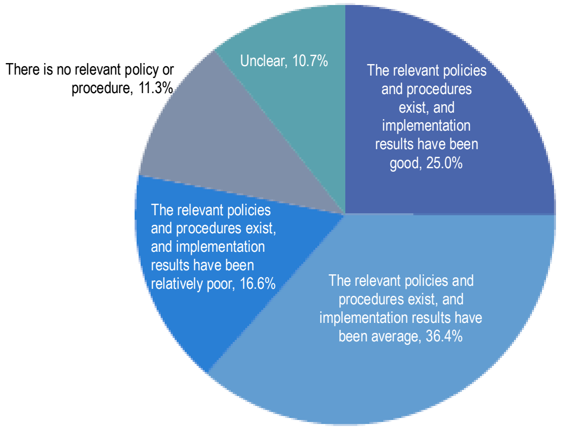


Figure 7-5 Establishment and implementation of cybersecurity management policies and procedures (sample size: 4,349)

From the perspective of industry, we find that internal cybersecurity policies and operating procedures tended to be more complete in finance (88.1%), energy (83.8%), and scientific research institutions and academies (82.1%) (see Figure 7-6).

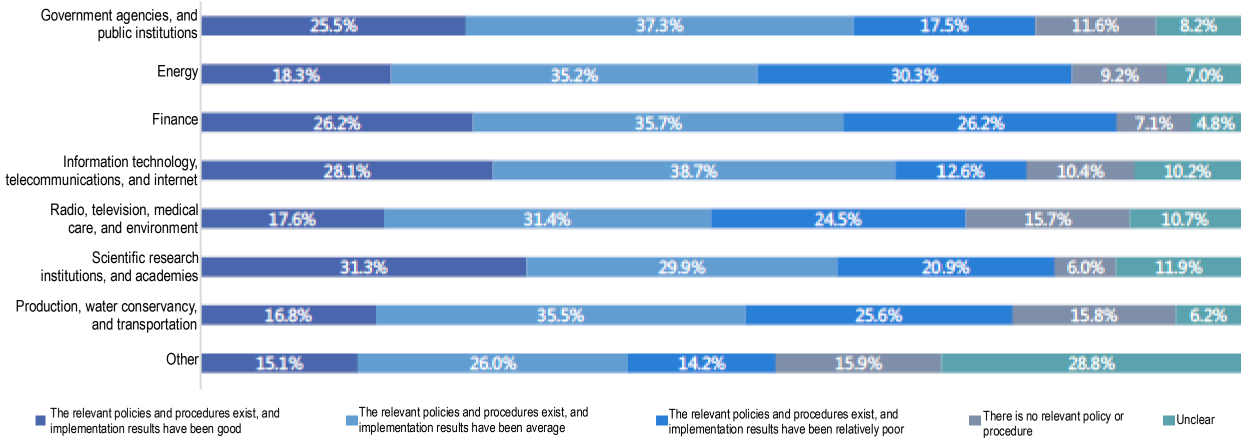


Figure 7-6 Establishment and implementation of cybersecurity management policies and procedures, by industry (sample size: 4,349)

From the perspective of work unit nature, we find that institutions of higher learning and scientific research institutes (86.2%), enterprises with foreign company investment (82.3%), SOEs (82.2%), and government agencies and public institutions had cybersecurity management policies and operating procedures that were more complete (see Figure 7-7).

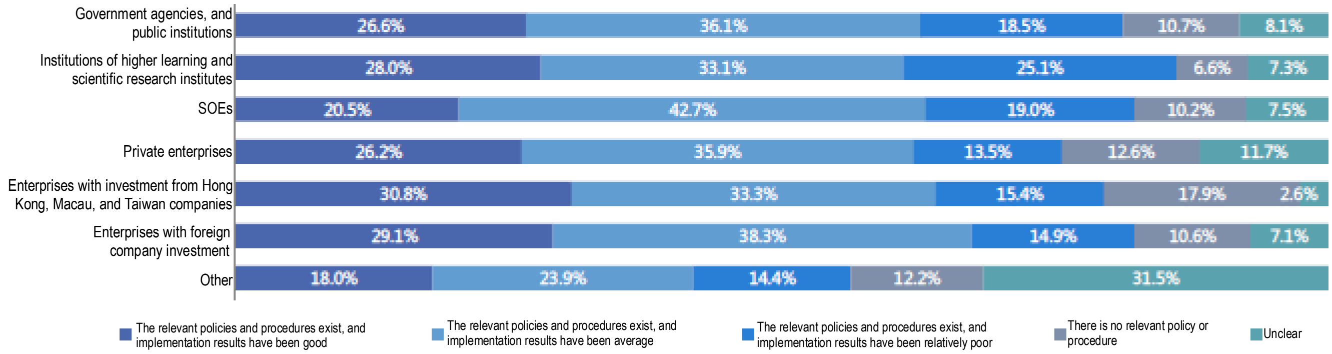


Figure 7-7 Establishment and implementation of cybersecurity management policies and procedures, by nature of work unit (sample size: 4,349)

From the perspective of work unit size, we find that the larger the employer, the more complete its internal cybersecurity management policies and operating procedures and the better its implementation results. 61.4% of employers with fewer than 20 employees had established the relevant policies and procedures, but more than 80% of employers with more than 1,000 employees had established the relevant policies and procedures. Moreover, 30% of the latter had obtained good implementation results, significantly higher than the mean (25%). In addition, more than 20% of employers with fewer than 20 employees had not set up cybersecurity management policies, yet only 6.6% of employers with more than 1,000 employees had not instituted the relevant policies (see Figure 7-8). Overall, the larger the employer, the greater the value placed on information security work and, correspondingly, the sounder were the information security management policies.

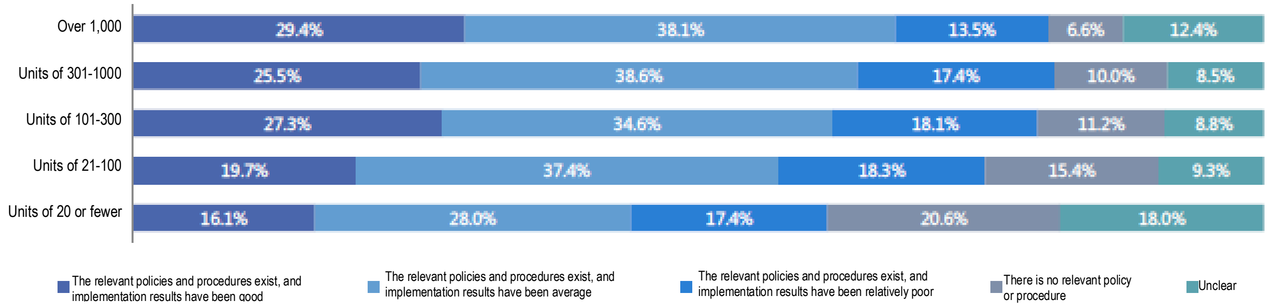


Figure 7-8 Establishment and implementation of cybersecurity management policies and procedures, by employer size (sample size: 4,349)

IV. More than seventy percent of units had begun information security risk evaluation work

Information security risk evaluation is a fundamental aspect of and important link in information security assurance work. It should be present throughout the entire process of network and information system building and operations. The state has established clear-cut rules for conducting information security risk evaluation work. These require analysis and evaluation of potential threats, weak links, and protective measures as they relate to network and information system security. The *Cybersecurity Law* stipulates that, at least once a year, critical information infrastructure operators shall conduct an inspection and assessment of their networks' security and possible risks, either on their own or by hiring a cybersecurity services organization.

According to the study data, 77.6% of practitioners stated that information security risk evaluation work was already underway in their units. This work was mainly "conducted by the unit itself," "by commissioning a third party," and "by a combination of the two" (see Figure 7-9).

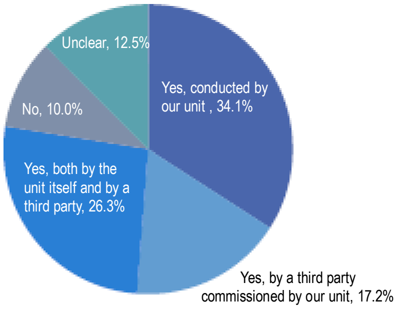


Figure 7-9 Status of information security risk evaluation work (sample size: 4,349)

IV. More than seventy percent of units had begun information security risk evaluation work

Compared to other industries, units in the information technology, telecommunications, and internet industry were more likely to conduct information security risk evaluation work on their own (see Figure 7-10).

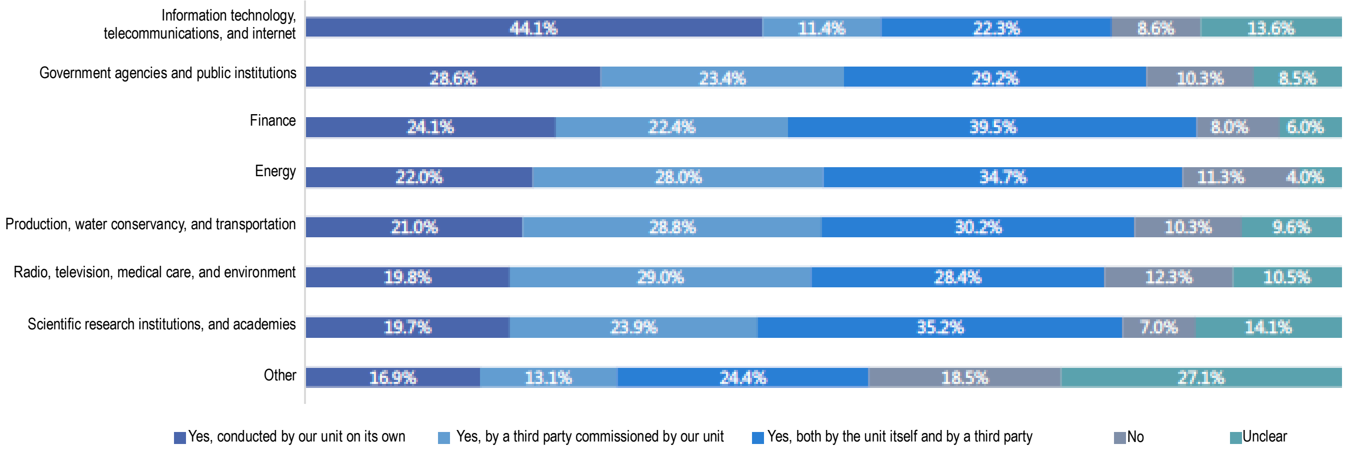


Figure 7-10 Status of information security risk evaluation work, by industry (sample size: 4,349)

V. Internal + Outsourcing Is the Main Way Units Dispose of Cybersecurity Threats

The main ways in which enterprises and public institutions disposed of cybersecurity threats were to resolve them with an internal security team (41.8%) or to resolve them through a combination of an internal team and outsourcing (43.0%). 11.6% resolved security matters entirely through a third party (see Figure 7-11).

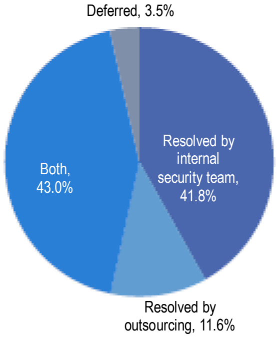


Figure 7-11 Manner of disposition of information security threats (sample size: 4,349)

From an industry perspective, we find that units in the information technology, telecommunications, and internet industry were more likely to adopt an internal security team approach to resolving threats (see Figure 7-12).

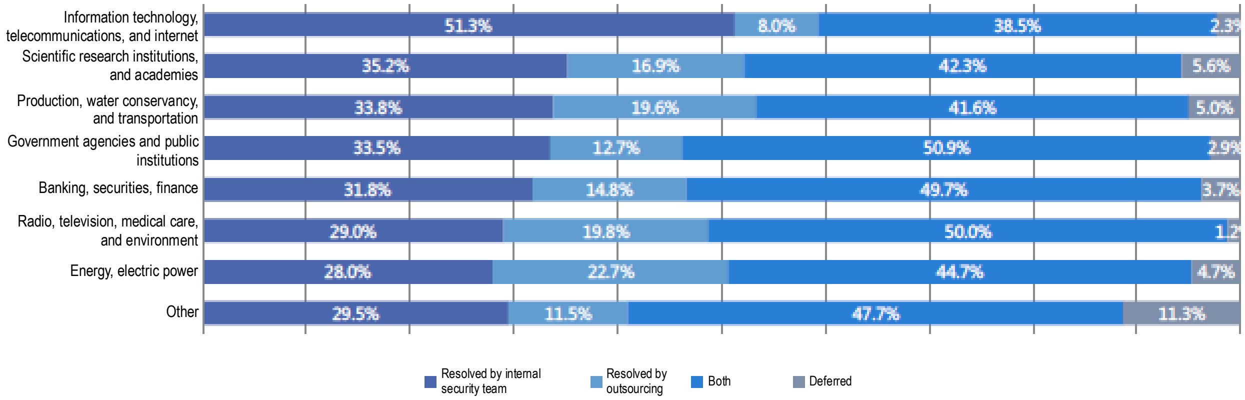


Figure 7-12 Manner of disposition of information security threats, by industry (sample size: 4,349)

In addition, the greater the size of the information security team, the more common it was to resolve cybersecurity threats with an internal team (see Figure 7-13).

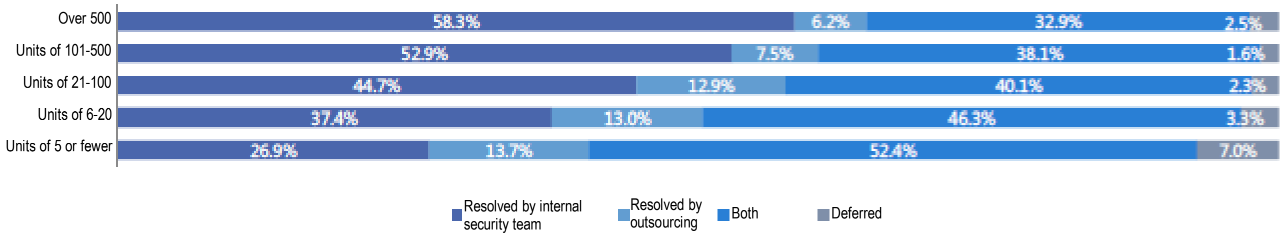


Figure 7-13 Manner of disposition of information security threats, by security team size (sample size: 4,349)

The greater the shortage of security practitioners at a unit, the more likely that it would adopt an internal and outsourcing approach to dispose of a cybersecurity threat (see Figure 7-14).

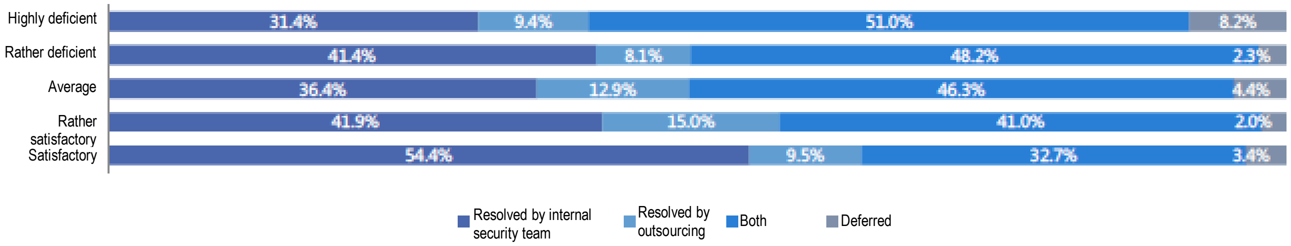


Figure 7-14 Manner of disposition of information security threats, by level of work unit security personnel shortage (sample size: 4,349)

VI. Big Data, Cloud Computing, IoT, Mobile Internet, and AI Are the Future Development Direction of the Information Security Industry

More than half of information security professionals believe that big data security, cloud computing security, AI security, IoT security, and mobile internet security are key development directions for the future of the security industry (see Figure 7-15).

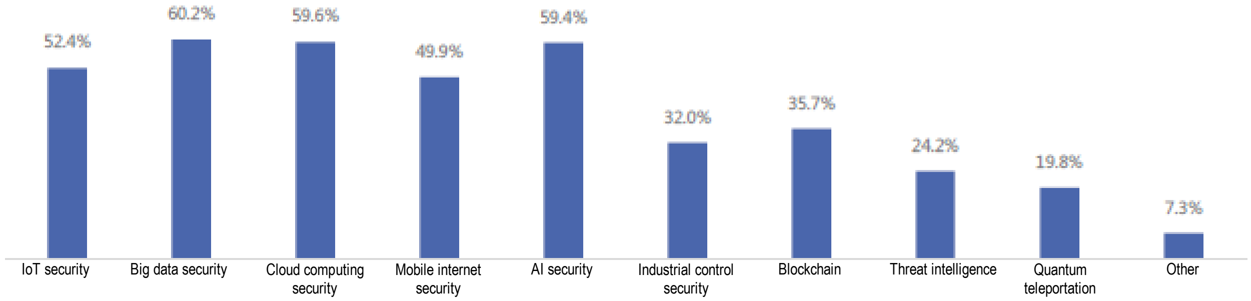


Figure 7-15 Respondent forecasts of future information security industry hot spots (sample size: 4,349)

VII. "Domestic Production of Chips" Is of the Greatest Importance to Building a Cyber powerhouse

Core technologies are pillars of the nation. They "cannot be exchanged on the market or bought with money," and we "must rely on our own R&D." In the study of the previous year, respondents believed that "domestic production of operating systems" was most important for building a cyber powerhouse. Under the impact of the "ZTE Incident," "domestic production of chips" replaced the previous year's "domestic production of operating systems" in this study as the option with the highest domestic production priority in the eyes of respondents this year. 40.3% of respondents believed that, with regard to building a cyber powerhouse, the domestic production need was greatest for chips, followed by operating systems (21.2%) and database systems (14.6%) (see Figure 7-16).

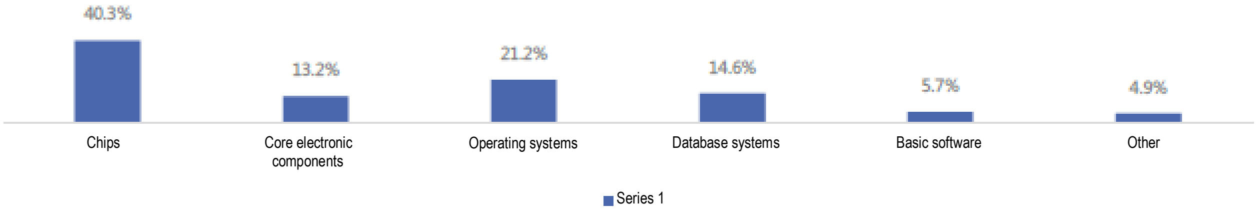


Figure 7-16 Technology most in need of domestic production for building cyber powerhouse according to

respondents (sample size: 4,349)

8. Study Conclusion

Cyberspace competition is, in the final analysis, a talent competition. Cyber and information security talent is urgently needed for the people's welfare and is an important resource in strategically contested fields. The building of information security talent teams is important, fundamental work for assuring national cyberspace security. Since the 18th Party Congress, the state has taken a series of important actions concerning the development of cybersecurity talent. It has introduced several powerful measures which have achieved successes that are obvious to all. Breakthrough progress has been made in establishing cybersecurity curricula, specializations, academic departments, and degree-granting programs. Cybersecurity has progressed rapidly in the areas of on-the-job training and professional certification testing. Cybersecurity attack-and-defense training exercises and skill competitions have seen vigorous growth. Cybersecurity talent and innovation bases have been planned and built in multiple locations to promulgate talent cultivation and recruitment policies. Important industries are strictly implementing cybersecurity responsibility systems and personnel compliance requirements while accelerating implementation of security personnel training and management regimes. The departments concerned launched in-depth propaganda and education efforts, significantly heightening cybersecurity consciousness throughout society.

However, it is clear that there remains a rather large gap between the current skill structure of information security talent teams and the needs of economic and social development and national security. China currently finds itself in a period of major strategic opportunity for cyber and information security talent development. In-depth research is necessary now and for a while into the future to track the current status of information security practitioner teams, to explore the growth patterns of information security talent, to analyze problems present at the deeper levels of the effort to build talent teams, and to provide decision-making references for information security talent-related work. This study shows that China's current effort to build information security talent teams still suffers from the following outstanding problems.

I. All-Around Shortage of Information Security Professionals

II. Professionalization of Information Security Is Still in the Initial Stages

III. Difficulty in Meeting the Demand for Personnel Ability Enhancement

IV. Impediments in Institutional Mechanisms for Information Security Talent

I. All-Around Shortage of Information Security Professionals

Whether it relates to a work layer such as data, applications, systems, or networks or to a business process such as R&D, system building, operations, management, or production, each link in the effort to informatize the entirety of information security work requires someone to assume information security work duties. However, there is at present an all-around shortage of information security professionals in China: **1) The total number of information security personnel is inadequate.** With the exception of information security professional service enterprises, huge enterprises and conglomerates, and large internet enterprises, all of which establish large information security talent teams, 50% of government and business units have information security teams with fewer than 20 members. The majority of respondents believe that the information security team at their own unit is too small to meet current work needs.

2) A large amount of information security work is completed on a part-time basis. Nearly six-tenths of information security professionals are required to do work that has no information security content. The phenomenon of requiring "multiple jobs for one person" is most significant in government agencies and public institutions. Among those who are required to perform additional non-security work, 33.8% of respondents said that non-security work accounted for more than 50% of their everyday work.

3) All types of security work roles suffer from talent shortages. From the perspective of security role major categories, we find the most severe shortages in the security development role and the planning and management role. As for subcategories, the roles with the worst shortages are, in order of severity, analysis design, organizational management, and development and integration. The deficiency of information security talent resources is one of the most important causes of information security incidents.

II. Professionalization of Information Security Is Still in the Initial Stages

Information security professionalization consists of the standardization of the professional knowledge, skills, and rules of conduct for information security professionals. An embodiment of professionalization is specialized personnel in specialized positions engaging in specialized work. China's *Cybersecurity Law* has already established clear requirements for "setting up specialized security management bodies and assigning persons in charge of security management" by critical information infrastructure operators. It also encourages other network operators to voluntarily participate in critical information infrastructure protection systems. The study shows that nearly seventy percent of work units where information security professionals were employed had set up specialized cybersecurity management departments and assigned persons to be in charge of cybersecurity management. However, overall, information security professionalization remains in the initial stages of development.

First, information security still lacks a unified professional (tribe) standard. Standards have yet to be established for such matters as how to rank and classify practitioners and what kind of professional knowledge and abilities they should have. Each employer sets up its own information security positions and sets its own requirements; the differences are quite large.

Second, the "personnel-post mismatch" is widespread in information security. Nearly seventy percent of work units where information security professionals were employed had set up specialized cybersecurity management departments and assigned persons to be in charge of cybersecurity management. However, 57.7% of the practitioners in units that had already established mechanisms were also responsible for other non-security work. The phenomenon of "personnel-post mismatch" is still quite widespread. In some cases, practitioners do not have the ability required by the position. In other cases, the job title is that of a specialized information security position, but the work actually done by the person filling the position is informatization or some other such work.

Third, societal awareness of information security occupations is weak, especially in employer senior management. Perhaps there needs to be a greater recognition of the importance of information security work and information security talent. Perhaps acknowledgment of the importance of talent work exists in principle only. We still do not know how to go about scientifically and effectively strengthening the work of building information security teams. More than half of practitioners believe that the failure to take information security work seriously on the part of administrators and senior management is one of the main reasons for security incidents.

III. Difficulty in Meeting the Demand for Personnel Ability Enhancement

Talent is the number-one resource. The core of strategic human resources management lies in viewing people as important assets and, through inputs such as education and training, continuously improving their knowledge, skills, and personal qualities so that they can better achieve the business goals of employers. The ability of employers to provide sufficient training, continuously improve the professional skills of talent, and help them to achieve self-realization of values will play an increasingly important role in "talent recruitment" and "talent retention." It is now universally difficult to meet the demand for personnel ability enhancement:

First, there is a thriving demand for practitioner ability enhancement. It is often necessary for newly hired personnel to receive "second training" following degree-granting education. Employed personnel also have a need for continuing education and lifelong learning. The study shows a rise in respondent demand for ability enhancement in each narrowly defined orientation of professional knowledge and ability. The areas in which they most wished to pursue professional ability enhancement were big data security, cloud security, security management, and penetration testing.

Second, practitioners expect to obtain professional credentials to serve as proof that they have a certain amount of knowledge, ability, and work experience. More than sixty percent (64.7%) of respondents had information security credentials of one type or another. Those holding a Certified Information Security Professional (CISP) credential accounted for the highest proportion (71.8%). 83.7% of practitioners expected to obtain an information security credential within the next year, and those among them who hoped to acquire a CISP credential accounted for the highest proportion (68.9%).

Third, employers do not invest enough in education and training. Information security personnel are generally "used much, trained little." Internal training systems are poorly implemented. 74.9% of work units where practitioners are employed established information security staff training systems, but only 23.1% of respondents believed the training obtained good results. At the same time, there has not been much willingness or effort on the part of employers to financially aid practitioners so that they can receive occupational training. Only 18.5% provided financial aid at 50% or more. 33.5% of practitioners stated that their own work units did not provide any financial aid.

IV. Impediments in Institutional Mechanisms for Information Security Talent

Cyber and information security is a non-traditional, interdisciplinary industry that crosses boundaries and merges with other industries. Thus, only institutional mechanisms that encourage innovative development can allow the creativity of talented people to compete and blossom and their ability and intelligence to gush forth. There still exist a series of institutional impediments to the development of information security talent.

First, the methods for assessing security practitioners are insufficient. Information security work is not very amenable to direct, quantitative assessment. It is difficult to embody information security results and values directly. 43.7% of information security professionals believed that their job title could not be clearly categorized. Many information security professionals experience difficulties within their institutions during job title evaluations, performance assessments, or selection and appointment.

Second, personnel incentive mechanisms are unsound, and opportunities for career advancement are limited. 65.5% of information security professionals stated that the personnel management department of their work unit established career advancement channels and work incentive mechanisms for information security professionals, but less than twenty percent believed that the relevant mechanisms had “good implementation results.”

Third, mechanisms for guiding talent to important and critical fields are lacking. In the midst of occupational mobility, practitioners attach great importance to both benefit and development-related factors. However, a large number of critical information infrastructure operators are facing challenges in such areas as “attractive pay” and “career retention.” Some are even experiencing relatively severe losses of their own talent.

9. Suggested Solutions

As the new S&T revolution continues and industries upgrade, information technology is fundamentally changing the way people live and shaping new patterns of economic and social development and national security. Information security talent will play a critical role in this process of transformative development. Given new challenges and opportunities, the question of whether information security talent development can be accelerated will become a major strategic issue bearing on whether we can gain the initiative in a setting of increasingly intense international competition.

The implementation of cyber powerhouse strategy deployments in the new era requires that we take Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, in particular his thinking on cyber powerhouse strategy, as the guide. We should place talent-related work in an even more prominent strategic position, further raise the importance and urgency of information security talent work, make use of our great power advantages and institutional advantages, and push forward with the effort to raise information security awareness and abilities throughout society and especially to enhance the skills of information security professionals. In light of the current situation of practitioners, this report puts forward the following recommendations for building information security teams.

I. Establishing a Systematic Information Security Talent Development Plan

II. Using Science to Push Forward Professionalization of Information Security Talent

III. Making an Effort to Improve the Numbers and Abilities of Information Security Professionals

IV. Continuously Optimizing the Overall Environment for Information Security Talent

I. Establishing a Systematic Information Security Talent Development Plan

From the high perspective of raising information age productivity, and making the building of globally competitive cybersecurity talent teams our goal, let us carry out systematic, advanced planning and deployments with regard to the overall situation of national cyber and information security talent development. Let us strive to seize the initiative and provide the materials for a solid foundation on which professional information security teams can be built.

First, build a cybersecurity national education and continuing education system. Provide overall guidance for all types of cybersecurity consciousness raising, basic education, advanced education, occupational training, and continuing education, and provide support for enhancing the information security abilities and protection skills of all members of society, including information security professionals, backup personnel, and the general public.

Second, make a unified plan to push forward with overall cybersecurity talent development work. Make an overall plan that includes all work relating to information security talent, including its cultivation, management, and use; clearly define major tasks and stage-by-stage goals; and accelerate reforms of information security talent management systems and work mechanisms such as those relating to personnel mobility and allocation, cultivation and development, performance assessment, and motivation assurance.

Third, with the collaboration of multiple entities, jointly build a cybersecurity talent ecosystem. Raise the intensity of support and cooperation among the leading departments concerned, industry, academia, scientific research institutes, employers, and other relevant parties; forcefully integrate resources, perfect supporting measures, and form a combined, driving force; jointly build a good ecosystem for developing cyber and information security talent.

II. Using Science to Push Forward Professionalization of Information Security Talent

Given the severe, all-around shortage of information security professionals, professionalization measures will help to make clear the legitimacy of information security occupations, increase the relevance of information security education and training, bring about a balance in information security talent supply and demand, and make information security occupations more attractive. However, since information security is an emerging, non-traditional field, professionalization should not entail a one-size-fits-all occupational licensing approach to managing the different types of practitioners in the field. Recommendations:

First, launch in-depth basic theoretical and cutting-edge practical research into information security talent development. Search for information security talent growth patterns, and create scientific testing and evaluation standards for information security professionals. Such standards will serve as a development basis for information security talent professionalization and will provide support for setting practitioner education and training goals and perfecting talent management systems.

Second, establish an information security knowledge system that is both relatively stable and dynamic. Synthesize the core and universal parts within the information security professional ability spectrum, and maintain a relatively stable basic knowledge system; establish dynamically adjusted knowledge subfields for narrowly defined orientations and cutting-edge fields to lay a solid foundation for information security professionalization.

Third, push forward information security professional talent credentialing work at authoritative institutions. Credentialing work conducted by trusted institutions can effectively prove that practitioners possess the appropriate professional knowledge and capabilities, work experience and achievements, and relatively high levels of professional ethics and thus provide a reference basis for talent performance assessment, selection and appointment, and career advancement as they relate to information security.

III. Making an Effort to Improve the Numbers and Abilities of Information Security Professionals

Guided by the needs of economic and social development and of national security, let us strengthen the farsightedness and relevance of the work of building a talent cultivation system, establish a lifelong education system that is involved throughout the work of information security practitioner learning, and improve the numbers and overall abilities of information security talent teams.

First, increase education and training inputs and work intensity. On the one hand, make proper use of mature occupational training systems to rapidly cultivate urgently needed information security talent. On the other hand, thoroughly push forward with cybersecurity education in basic education, advanced education, and vocational schools so as to actively cultivate information security reserve talent. Comprehensively optimize the content, categories, hierarchical structure, and industry-related distribution of education and training. Make an effort to solve the outstanding problem of an overall shortage of information security talent.

Second, take differentiated measures to build information security talent teams. With regard to society's need for information security entry-level personnel, foster such personnel on a large scale to meet current employment needs as soon as possible. As for the need for outstanding engineers and high-level researchers, strengthen specialized training on a foundation of engineering and scientific research projects in order to shape information security key task teams and backbone forces. As for the need for information security core technology talent and special talent, explore special cultivation and selection schemes to form core and critical information security abilities.

Third, push forward with information security education and training supply-side reforms in light of the characteristics of specific fields. Strengthen the leading and guiding roles of professional certification testing in building talent teams, innovate talent cultivation models, deepen industry-education collaboration, open up reserve talent-to-practitioner channels, and push all types of schools, professional training institutions, and enterprises to promote high-quality development of information security talent work through campus education, modern apprenticeship training, orientation training, on-the-job training, on-the-job drills, attack-and-defense competitions, technological contests, and other approaches.

IV. Continuously Optimizing the Overall Environment for Information Security Talent

Cybersecurity is a cutting-edge field of information technology. It is the field with the greatest concentration of intellectual power and the greatest need for innovation vitality. Let us hold fast to the principles of pragmatism, give priority to urgent needs, and accelerate innovations in institutional mechanisms for developing information security talent. Formulate talent policies adapted to information security characteristics, and allow the creativity of talented people to compete and blossom and their ability and intelligence to gush forth.

First, raise the cybersecurity consciousness and cybersecurity talent consciousness of leading Party and government cadres at all levels. Make cybersecurity a mandatory course in cadre training, guide their enthusiasm to meet the requirements of the present age, strengthen their cybersecurity mindset so that they better understand the importance of talent work, truly respect talent, cherish talent, and create good conditions for talent development.

Second, accelerate innovation of evaluation and incentive mechanisms for information security professionals. Drawing on the best management practices and experiences for arousing the vitality of information security talent in enterprises, innovate and develop salary regimes, evaluation indices, and incentive mechanisms adapted to information security characteristics, respect and embody information security talent values, and legitimately raise the pay and social position of practitioners.

Third, establish information security talent guidance and priority assurance mechanisms for key fields. Adopt special policies and perfect supporting measures to guide and encourage the flow of information security talent to national Party and government agencies, vital sectors, important industries, and critical information infrastructure operators; ensure that key fields can recruit, employ, and retain top talent and talent in short supply.

10. Sample Demographics

I. Gender

The male-to-female ratio among Chinese information security professionals remains quite high. There are higher percentages of female practitioners involved in security situation analysis and strategic planning work roles and lower percentages in the security development and operations and maintenance work roles.

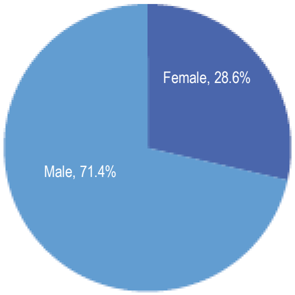


Figure 10-1 Respondent gender (sample size: 4,349)

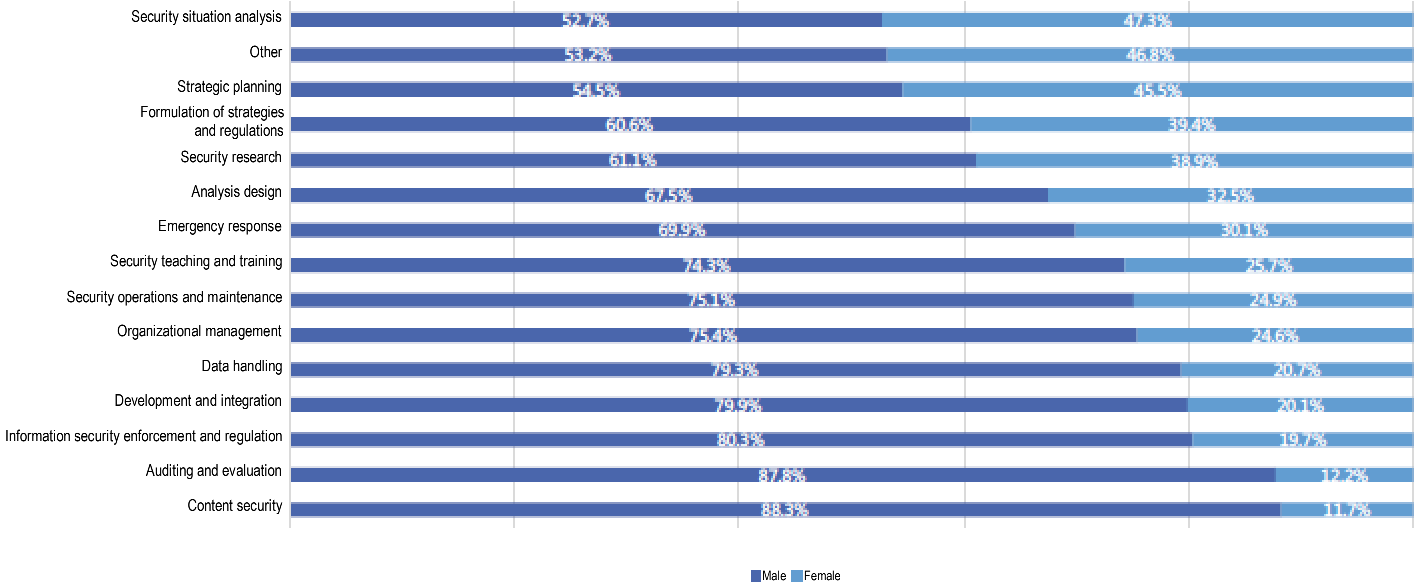


Figure 10-2 Respondent gender, by work role (sample size: 4,349)

II. Age

The age composition of information security professionals is relatively young. Young practitioners in the 20-40 age bracket are still the main force (88.3%). There was basically no change from the previous year (88.4%).

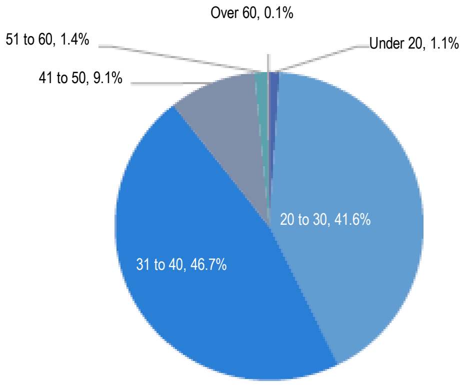


Figure 10-3 Respondent age (sample size: 4,349)

III. Educational Background

More than half of information security professionals have backgrounds in computer-related majors. Roughly 22.2% of security practitioners come from cyber and information security-related majors, slightly less than practitioners with non-computer-related majors (23.4%).

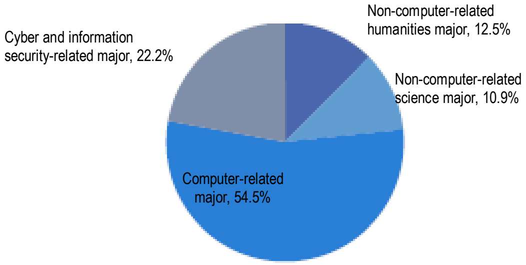


Figure 10-4 Major of respondent highest academic degree (sample size: 4,349)

IV. Highest Academic Degree

The overall academic degree level of information security professionals in China remained mainly at or above undergraduate (81.2%). Undergraduate degrees account for 65.0%, a slight increase over the study result of the previous year.

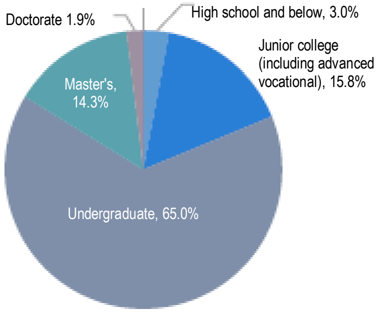


Figure 10-5 Respondent academic degree (sample size: 4,349)

V. Regional Distribution

This study included information security professionals from all provinces and regions of China. Nearly one-half (47.6%) of information security professionals came from first-tier cities such as Beijing, Shanghai, Guangzhou, and Shenzhen.

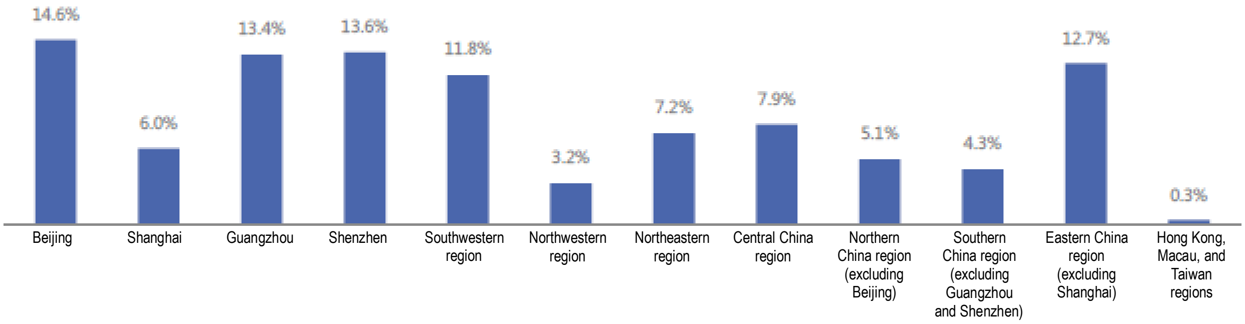


Figure 10-6 Respondent locality (sample size: 4344)