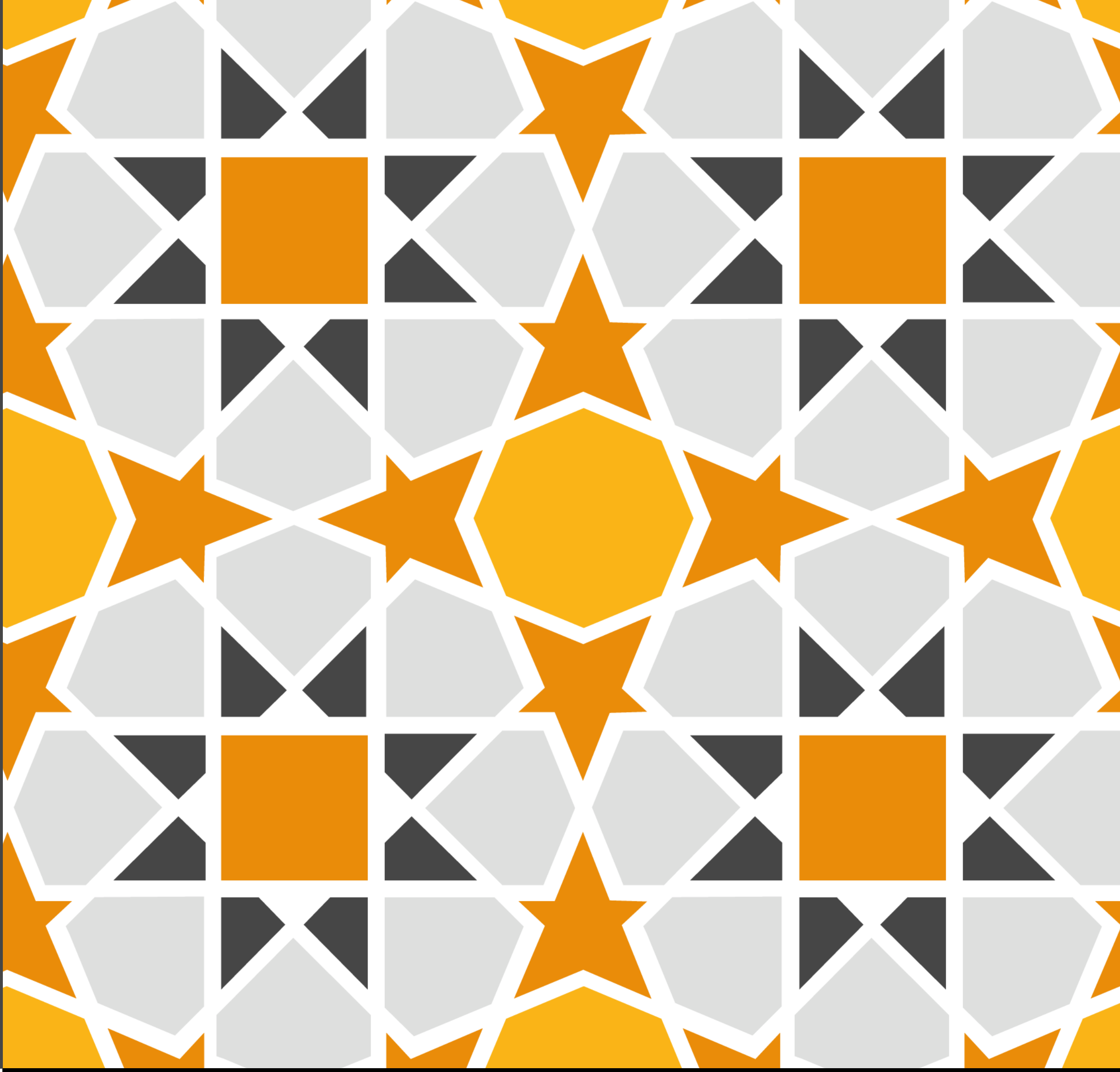


Career path survey in the Cybersecurity and Privacy industry 2024

pwc

www.pwc.com/jp/en

Table of Contents

1. Introduction

1. Introduction

Have you ever pictured yourself working in the cybersecurity industry?

Today, the digitalisation of business, which includes digital transformation and the use of artificial intelligence (AI), is spreading globally. As it spreads, business demand is growing for cybersecurity and privacy (hereinafter referred to as ‘cybersecurity’) industry services that protect information assets and human rights from increasingly sophisticated cyber threats. The demand for professionals behind these services is also increasing proportionally. Thus, the cybersecurity industry wants many talented and promising university students and mid-career changers who possess experience in other specialized fields.

However, the cybersecurity industry has not been around long, and people often lack a firm understanding of the field. What kind of people work in this industry? What backgrounds do they have? What kind of work do they do? In response to such questions, we have conducted a survey investigating the career paths of professionals working in the cybersecurity industry since 2022. Our intent is to help university students and people looking to make a career change get a clearer picture of themselves working in the industry. With this year’s survey on cybersecurity industry trends—the second conducted thus far—we expanded our scope to include not only cybersecurity professionals in Japan but also those in the US, a leader in the industry. We obtained responses from 600 cybersecurity professionals (300 males and 300 females).

We sincerely hope that our survey will inspire you to consider a career in the cybersecurity industry.

*For information on the 2022 survey, please refer to Women’s Career Path in the Cybersecurity and Privacy Industry 2022 (hereinafter the ‘First Career Path Survey’).

2. Twelve trends of professionals working in the US and Japanese cybersecurity industries

2. Twelve trends of professionals working in the US and Japanese cybersecurity industries

Through the survey, we identified 12 trends among professionals working in the cybersecurity industries in the US and Japan (Figure 1). Aligning the survey with the World Day for Cultural Diversity for Dialogue and Development[1],we analyzed the career paths of professionals working in the cybersecurity industry based on various group attributes. These include ‘Japan-US’, ‘gender’, ‘last degree earned (non-STEM or STEM)’, ‘experience/no experience with career change’ and ‘presence/absence of a role model’.

Figure 1: Twelve trends among professionals working in the US and Japanese cybersecurity industries

1. A high percentage of Japanese and US professionals working in the cybersecurity industry have ‘non-STEM’ backgrounds.
2. The most common previous industries for mid-career changers, in order, are ‘IT/cybersecurity vendors’, ‘manufacturing’, ‘service’ and ‘finance/insurance’.
3. ‘Sales department’ was at the top for professionals with non-STEM backgrounds who changed careers or departments, while ‘information cybersecurity department’ was at the top for professionals with STEM backgrounds.
4. The percentage of females in the cybersecurity industry is slowly rising.
5. Professionals with non-STEM backgrounds tend to be in ‘governance management’ , while those from STEM backgrounds tend to be in ‘engineering’.
6. The top impressions after working in the cybersecurity industry: ‘An industry that allows the development of expertise. ’
7. Seventy percent of Japanese and US professionals have role models. Many of them rated their work satisfaction positively, saying they are ‘satisfied with cybersecurity work’.
8. The top ‘definition of successful’ as considered by professionals is ‘being able to produce high-quality results efficiently within a given time frame’. However, there is a divergence with the top definition as expected within the company, which is ‘being in management’.
9. ‘Cloud security-related certification’ stands at the top of certifications ‘most useful for work’.
10. Eighty percent of Japanese and US professionals with role models ‘want to work in the cybersecurity industry for a long time’.
11. Most US professionals (more than 80%) want to be promoted. This number is higher than that of Japanese professionals.
12. Experience in ‘IT and cybersecurity practice’ and ‘consulting’ is the most beneficial for a person wishing to become a cybersecurity-related CxO [Chief x Officer].

[1] United Nations, “World Day for Cultural Diversity for Dialogue and Development, 21 May” https://www.un.org/en/observances/cultural-diversity-day

Past trends

What is most noteworthy in the survey's 'past trends' is the observation of similar trends in Japan and the US in regard to the last degree earned and the industry/organisational department of the previous jobs of cybersecurity professionals.

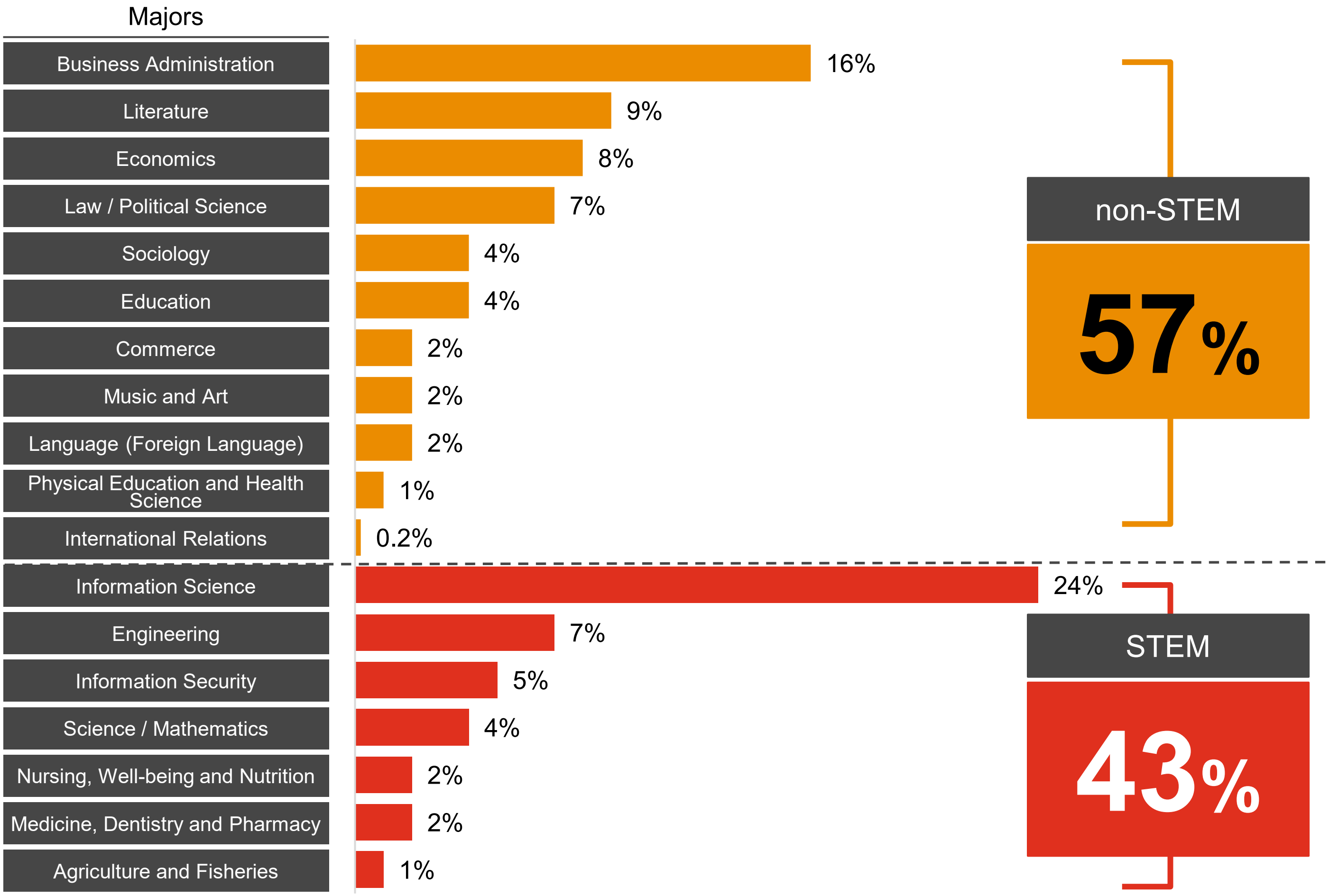
(1) A high percentage of Japanese and US professionals working in the cybersecurity industry have 'non-STEM' backgrounds.

Looking at the majors of professionals' 'last degree earned' (university or graduate school), it is clear that many 'professionals with non-STEM backgrounds' are active in the industry. Among Japanese and US cybersecurity professionals (n=582), approximately 60% had non-STEM backgrounds and 40% had STEM backgrounds (see Figure 2).

Looking specifically at the majors of professionals with non-STEM backgrounds, the most common were 'business administration' at 16%, followed by 'literature' (9%), 'economics' (8%), 'law/political science' (7%), 'sociology' (4%) and 'education' (4%). Looking next at the majors of professionals with STEM backgrounds, the most common were 'information science' at 24%, followed by 'engineering' (7%), 'information security' (5%) and 'science/mathematics' (4%).

From these figures, we can see that careers as cybersecurity professionals are open to both non-STEM majors and STEM majors, and that people with backgrounds in information science and business administration are particularly conspicuous among cybersecurity professionals in Japan and the US.

Figure 2: Majors of the final degree earned by professionals working in the cybersecurity industries of Japan and the US (n=582)

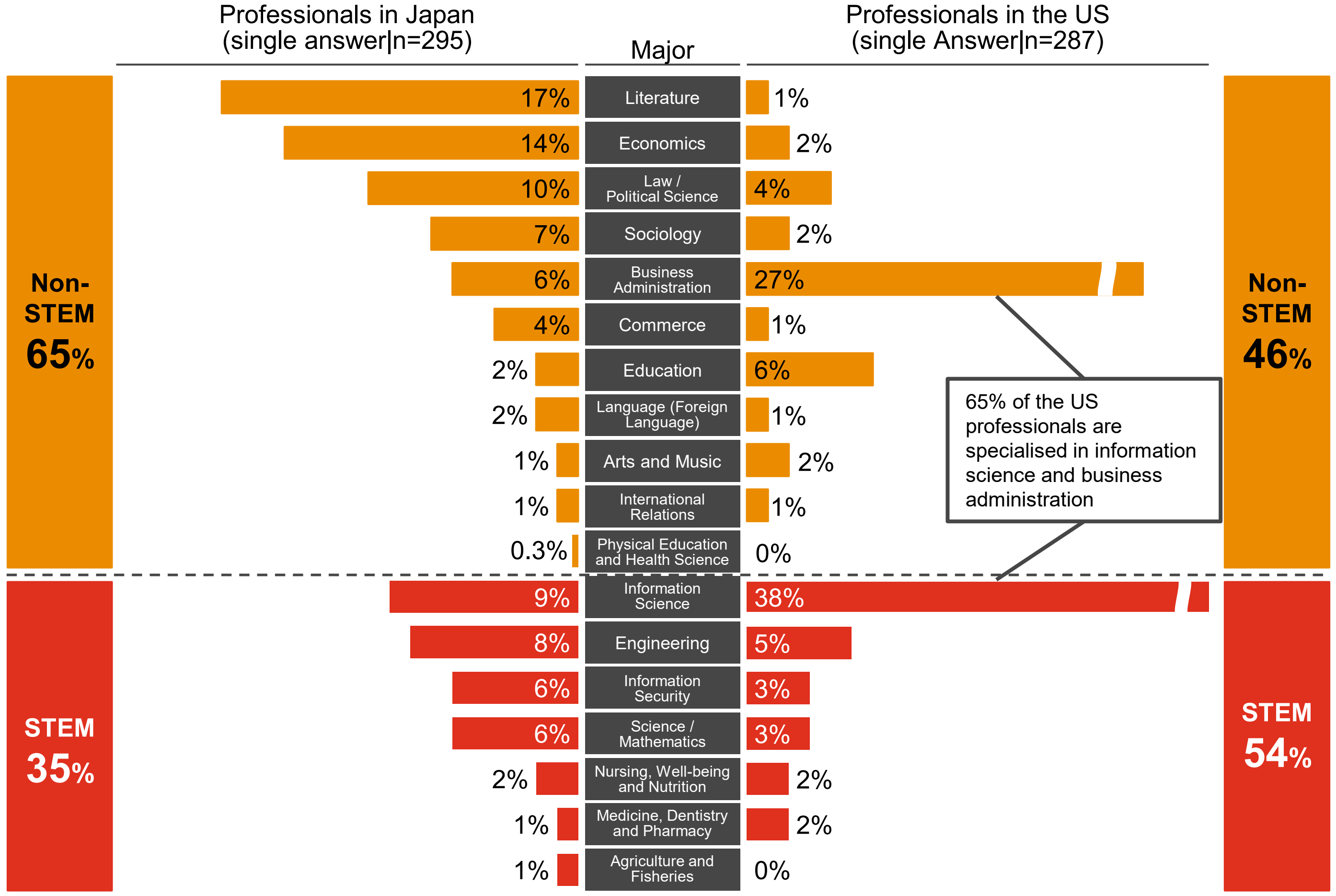


Q. What was your major in your final level of education?

Next, comparing Japanese and US professionals by country reveals that, among Japanese professionals (n=295), a higher percentage had non-STEM backgrounds, with 65% having non-STEM backgrounds and 35% having STEM backgrounds. On the other hand, the percentages were roughly the same among US professionals (n=287), with 46% having non-STEM backgrounds and 54% having STEM backgrounds (Figure 3). Furthermore, comparing the two countries by gender shows that the percentage of Japanese females with non-STEM backgrounds was higher than the percentages of the other groups (Japanese males 56%, US females 55% and US males 38%) at 74% (Figure 4 and Figure 5).

Looking specifically at the top five majors in each country, ‘literature’ was the most common among Japanese professionals at 17%, followed by ‘economics’ (14%), ‘law/political science’ (10%), ‘information science’ (9%) and ‘engineering’ (8%), indicating that the top three majors were non-STEM. Compared to the First Career Path Survey conducted two years ago, the ranking of ‘engineering’ shifted, but the top-ranking majors trended about the same, with the 2024 Industry Survey showing a higher percentage of professionals with non-STEM backgrounds. (First Career Path Survey: Among Japanese professionals, ‘engineering’ was the most common at 26%, followed by ‘literature’ [16%], ‘science’ [13%], ‘economics’ [12%] and ‘law/political science’ and ‘sociology’ [6% each].) A look at the top five majors among US professionals reveals that ‘information science’ was the most common at 38%, followed by ‘business administration’ (27%), ‘education’ (6%), ‘engineering’ (5%) and ‘law/political science’ (4%).

Figure 3: Majors of last degree earned by professionals working in the cybersecurity industries of Japan and the US (Japan-US comparison; n=582)

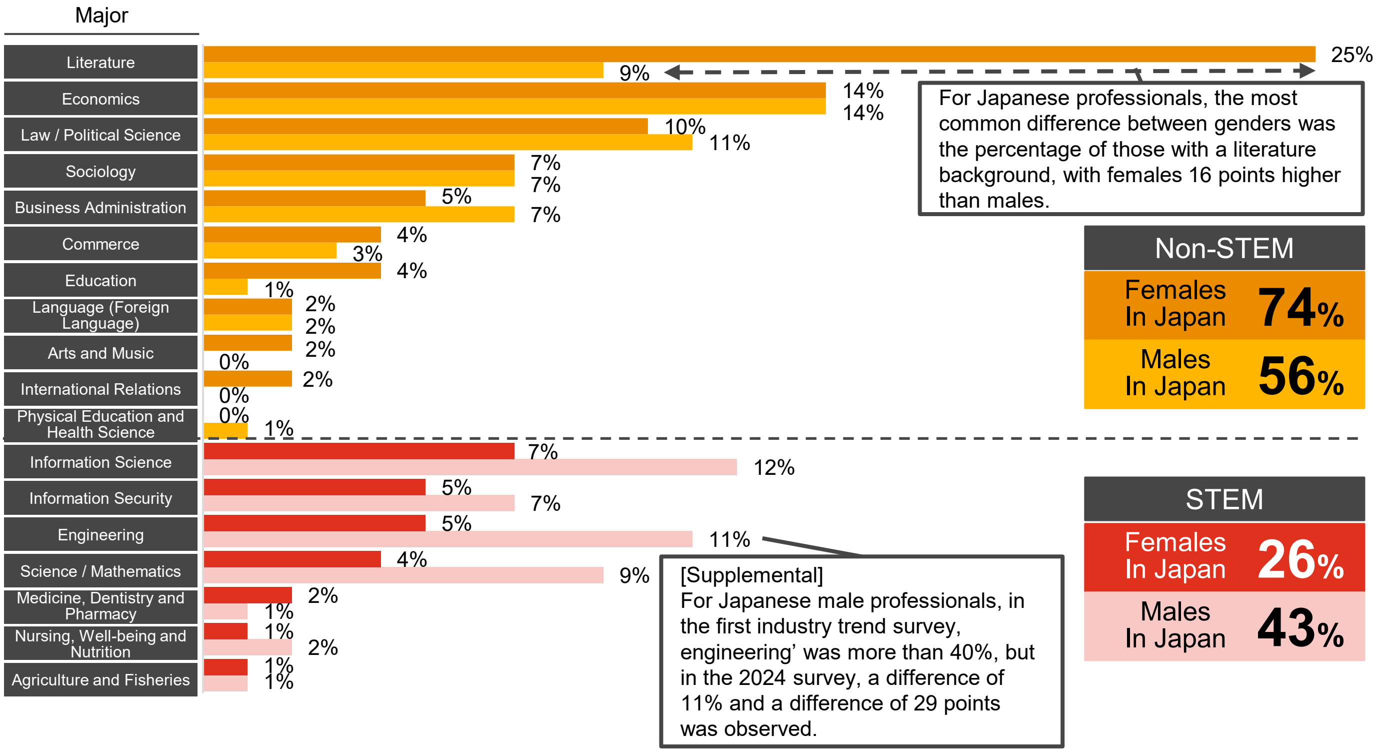


Q. Please let us know your field of study in your final level of education.

[Additional Note] In this survey, no US experts majoring in ‘Physical Education and Health Science’ or ‘Agriculture and Fisheries’ were identified.

These findings suggest that while Japanese professionals enter the industry from a wide range of majors, students in the US who wish to enter the cybersecurity industry should major in ‘information science/information cybersecurity science’ or ‘business administration’.

Figure 4: Majors of the final degree earned (Japan: gender comparison; males n=148, females n=147)



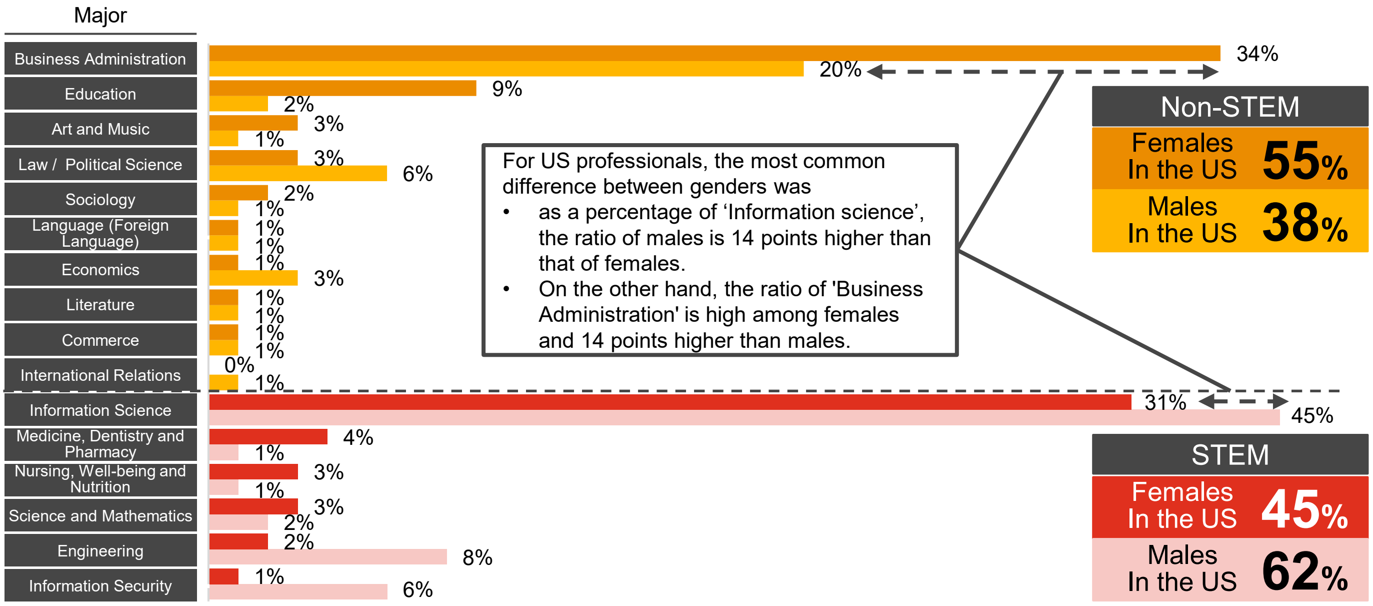
For Japanese professionals, the most common difference between genders was the percentage of those with a literature background, with females 16 points higher than males.

Non-STEM
Females In Japan 74%
Males In Japan 56%

STEM
Females In Japan 26%
Males In Japan 43%

[Supplemental]
For Japanese male professionals, in the first industry trend survey, engineering' was more than 40%, but in the 2024 survey, a difference of 11% and a difference of 29 points was observed.

Figure 5: Majors of the final degree earned (US: gender comparison; males n=144, females n=143)



For US professionals, the most common difference between genders was

- as a percentage of ‘Information science’, the ratio of males is 14 points higher than that of females.
- On the other hand, the ratio of 'Business Administration' is high among females and 14 points higher than males.

Non-STEM
Females In the US 55%
Males In the US 38%

STEM
Females In the US 45%
Males In the US 62%

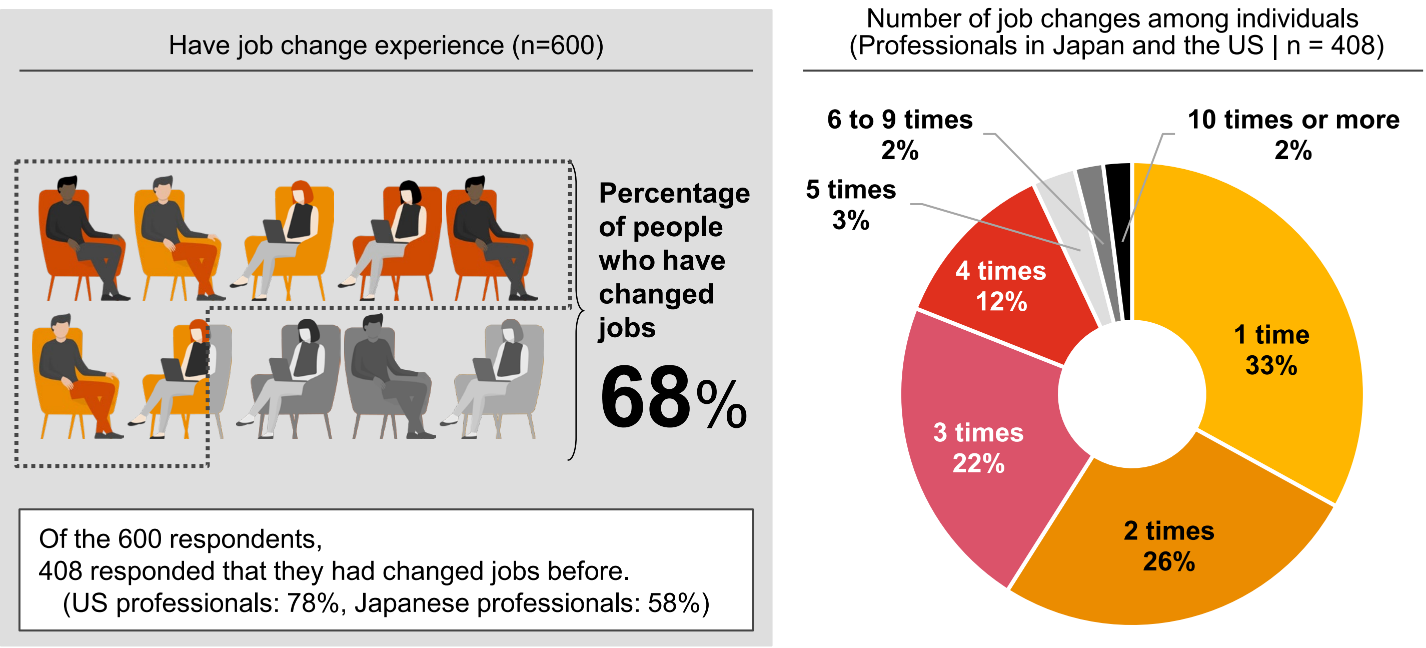
[Supplemental] In this survey, it was not possible to confirm the majors of 'Physical Education and Health Science' and 'Farming Science and Fisheries Science' of US professionals.

(2) The most common previous industries for mid-career changers, in order, are ‘IT/security vendors’, ‘manufacturing’, ‘service’ and ‘finance/insurance’.

Next, let’s look at respondents who have experienced a career change or a change of organisational departments.

When we asked Japanese and US professionals (n=600) about their experience in changing careers, 70% indicated that they had changed careers before (Figure 6). The percentage of US professionals who had changed careers was conspicuously high at 78%—20 percentage points higher than that of Japanese professionals (58%). When we asked the Japanese and US professionals who had changed careers (n=408) about the number of times they had done it, those indicating that they had changed careers two or more times made up the majority at 65%.

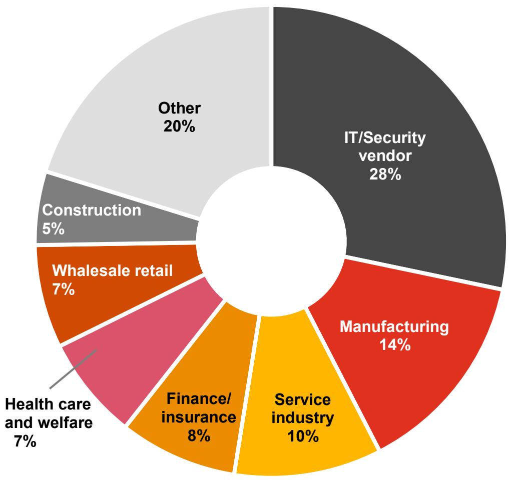
Figure 6: Percentages of Japanese and US professionals who have changed careers and number of career changes



When we asked those who had changed careers or departments (n=426) about the industry or organisational department of their previous job (or before their transfer), we found that ‘IT/security vendor’ was the most common at 30%, followed by ‘manufacturing’, ‘service’ and ‘finance/insurance’, in that order (Figure 7, left). Although there was no significant difference between Japanese and US professionals in terms of previous job industries, about half (43%) of the professionals with STEM backgrounds changed careers after working at an ‘IT/security vendor’. This figure was 26 percentage points higher than those with non-STEM backgrounds (17%) (Figure 7, right).

Figure 7: Previous job industries of respondents who changed careers or transferred to a new department

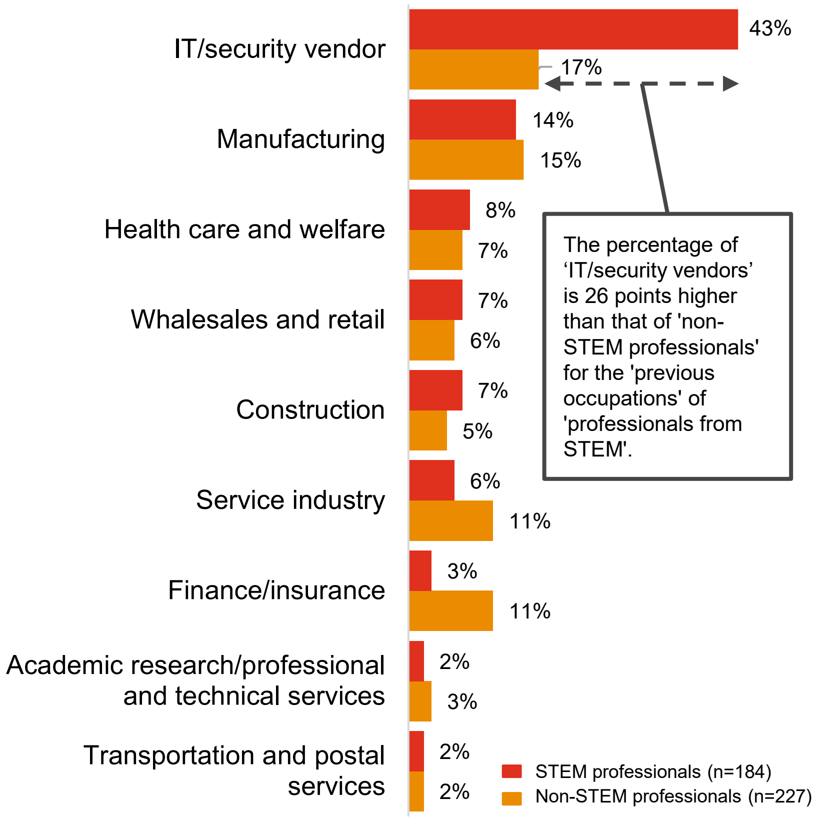
Previous job type(individuals who changed jobs and transferred departments|n=426)



There was no significant difference between Japan and the US in the type of occupation and previous job. The majority were IT and security vendors.

Q. Please tell us about the company you worked for before one and the type of industry you work in.

Top 10 industries in the previous job category (Major comparison|non-STEM n=227, STEM n=184)



The percentage of ‘IT/security vendors’ is 26 points higher than that of 'non-STEM professionals' for the 'previous occupations' of 'professionals from STEM'.

(3) ‘Sales department’ was at the top for professionals with non-STEM backgrounds who changed careers or departments, while ‘information security department’ was at the top for professionals with STEM backgrounds.

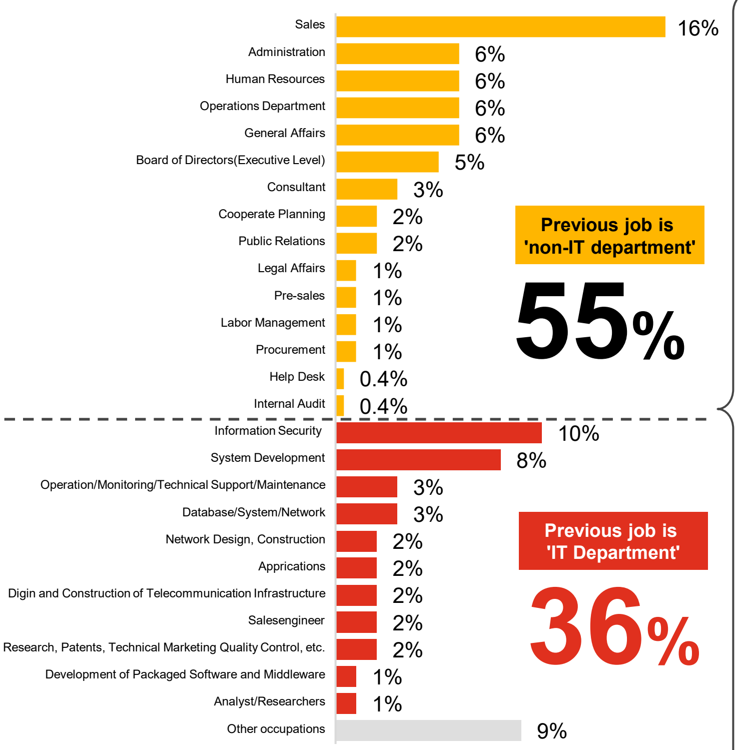
Looking at the organisational departments of the previous job or before transfer to a new department, approximately 60% were from ‘non-IT departments’ and 40% were from ‘IT departments’. This finding is a reversal of the results of the First Career Path Survey , which targeted Japan only and indicated a trend towards a higher percentage of respondents coming from ‘non-IT departments’ (Figure 8, left).

Looking specifically at the ‘non-IT department’ category, ‘sales department’ was the most common response at 16%, followed by ‘administration’, ‘human resources’, ‘operations department’ and ‘general affairs’ at 6% each and ‘board of directors (executive level)’ at 5%. In the ‘IT department’ category, ‘information security’ was the most common at 10%, followed by ‘system development’ at 8% and ‘operation/monitoring/technical support/maintenance’ and ‘database/system/network’ at 3% each.

Comparing these findings in terms of professionals with non-STEM backgrounds (n=267) and those with STEM backgrounds (n=217), the largest difference was found in ‘sales’,’ where 23% of professionals came with non-STEM backgrounds, compared to 5% of professionals with STEM backgrounds, a difference of 18 percentage points. Furthermore, a 14-percentage-point difference was observed in ‘information security’,’ where 18% of professionals came with STEM backgrounds, compared to 4% of professionals with non-STEM backgrounds.

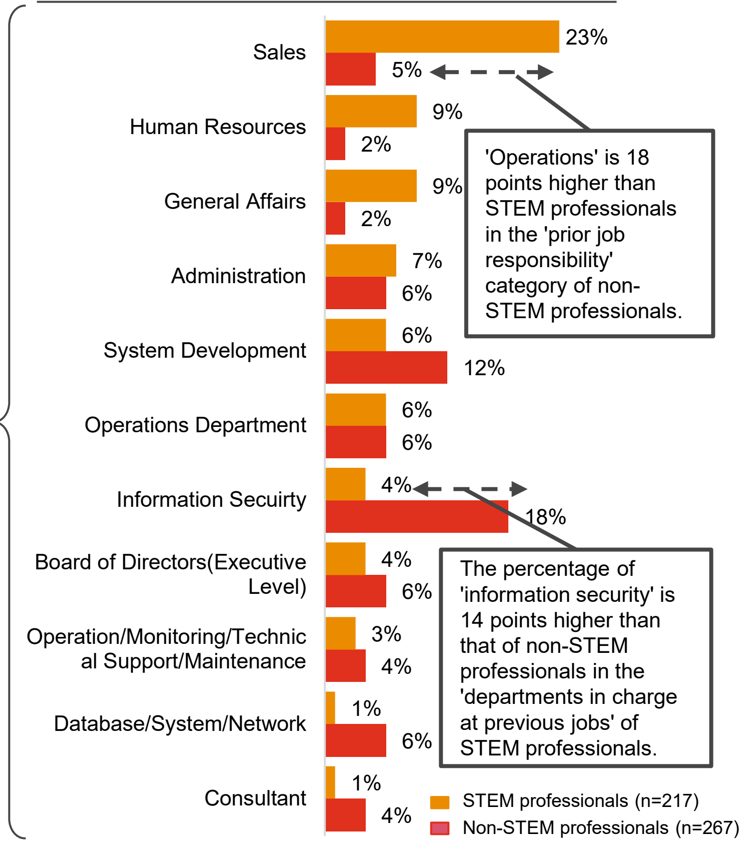
Figure 8: Previous job departments of respondents who changed jobs or transferred to a new department

Departments in charge at previous jobs (employees who have changed jobs or transferred to another department|n=499)



Q. If you had a previous job (job change experience or department transfer), please tell us the job type of your previous job.

Top 11 departments in the former division (comparison of STEM and non-STEM|n=484)



'Operations' is 18 points higher than STEM professionals in the 'prior job responsibility' category of non-STEM professionals.

The percentage of 'information security' is 14 points higher than that of non-STEM professionals in the 'departments in charge at previous jobs' of STEM professionals.

2. In the First Career Path Survey shows percentage coming from IT departments (50%), not-IT departments(42%) and Others(8%).

Current trends

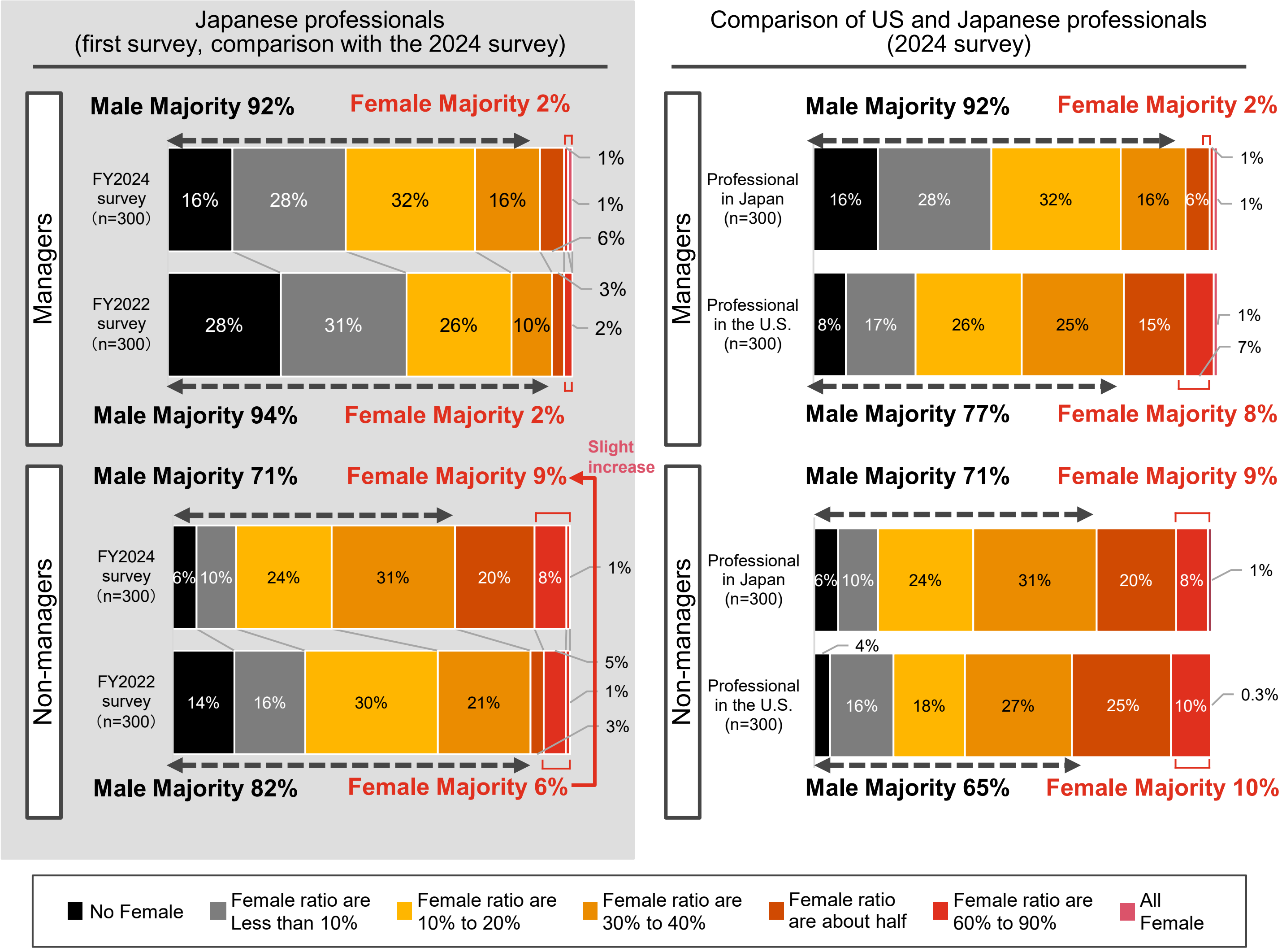
In the previous chapter, we examined past trends in cybersecurity professionals' career paths. In this chapter, we will look at the current trends.

(4) The percentage of females in the cybersecurity industry is slowly rising.

The number of female professionals in Japan's cybersecurity industry is said to be low, and the First Career Path Survey provided data confirming that trend.

This year's survey asked Japanese and US professionals (n=600) about the 'percentage of females in cybersecurity and privacy work' in their workplaces and found that the percentage of females has been gradually increasing in Japan since the First Career Path Survey conducted two years ago (Figure 9, left). In the US, the percentage is slightly higher than in Japan, but the industry is still dominated by males (Figure 9, right).

Figure 9: Percentages of females in cybersecurity and privacy work in Japanese and US workplaces

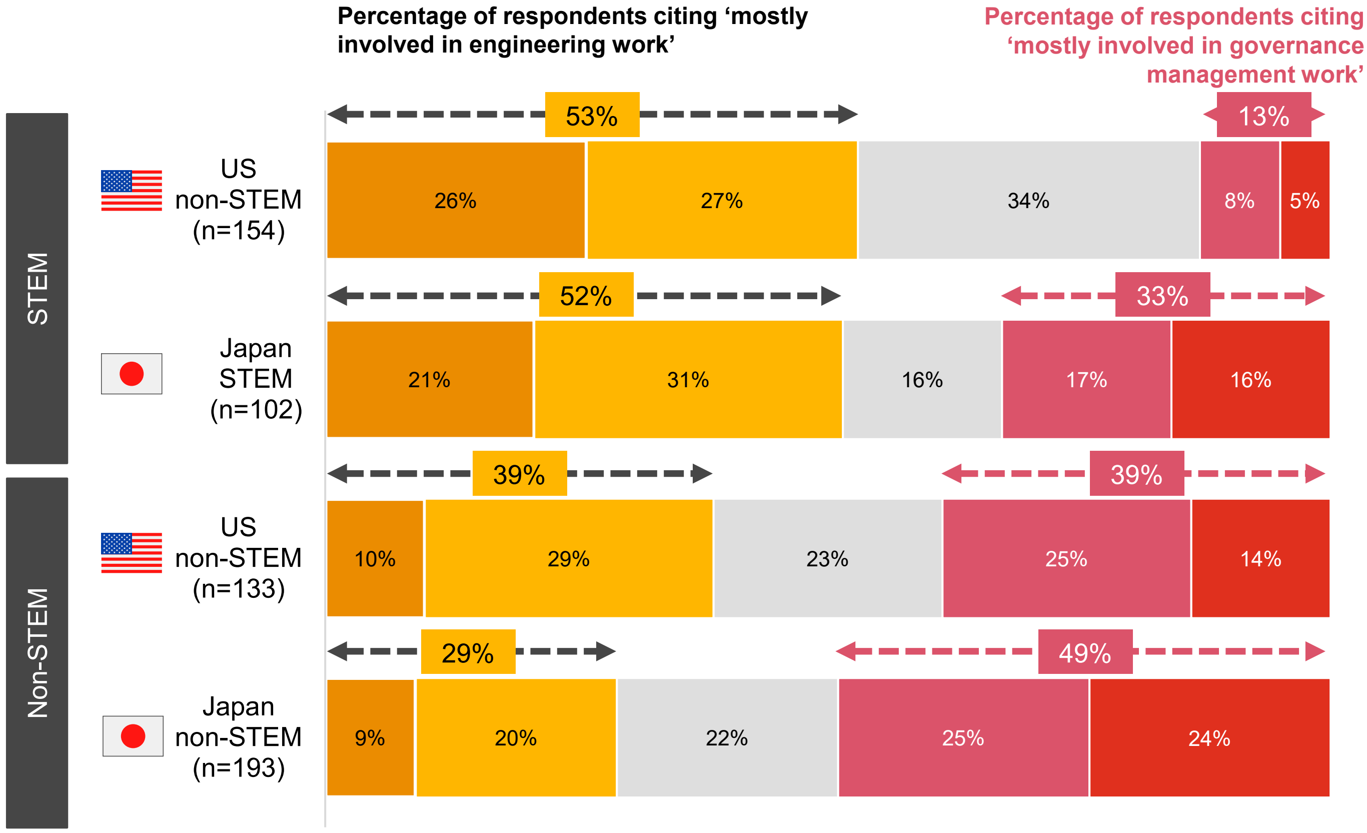


Q. Please tell us the percentage of women in your workplace who are involved in cybersecurity and privacy activities (managers or higher/non-managers).

(5) Professionals with non-STEM backgrounds tend to be in ‘governance management’, while those from STEM backgrounds tend to be in ‘engineering’.

While examining ‘current trends’ in the career paths of Japanese and US professionals, we identified trends in ‘area of work’ in the ‘major of last degree earned’ groups (STEM and non-STEM) (Figure 10). The percentage of professionals with STEM backgrounds who said they were ‘mostly involved in engineering work’ was high, accounting for a majority in both Japan and the US. However, a comparison between Japan and the US shows that the percentage of professionals who said they were ‘mostly involved in governance management work’ was 33% in Japan—20 percentage points higher than those who gave the same response in the US. In addition, professionals with non-STEM backgrounds were more likely than those with STEM backgrounds to say that they were ‘mostly involved in governance management work’ in both Japan and the US, with professionals with non-STEM backgrounds in Japan accounting for about 50% of the total—the highest percentage among all respondents.

Figure 10: ‘Percentages of involvement in engineering work and non-engineering (governance management) work’ among Japanese and US professionals (comparison of major of last degree earned groups)



🟧 All ‘engineering tasks7

🟨 Majority ‘engineering tasks’

⬜ ‘Engineering’ and ‘non-engineering (governance management) tasks’ are the same level.

🟥 Majority ‘non-engineering (governance management) tasks’

🟥 All ‘non-engineering (governance management) tasks’

In this context, engineering refers primarily to businesses that use engineering techniques (design, development, testing, operation, maintenance and R&D) for cybersecurity and privacy work. Non-engineering refers to work that primarily uses management and governance techniques for cybersecurity and privacy operations.

Q. Is the main business at your current location engineering or non-engineering (governance management) service? What is the most applicable?

Furthermore, looking at the timeline of ‘past’, ‘present’ and ‘future’ for specific work tasks, 80% of Japanese and US professionals had some experience in cybersecurity or privacy work in the past. Additionally, excluding US professionals with non-STEM backgrounds, 80% of Japanese and US professionals hoped to be doing cybersecurity work in the future. These findings indicate that the respondents are building career paths related to cybersecurity work (Figure 11).

Figure 11: Current work tasks (multiple responses accepted; n=600)

	Past						Present						Future					
	The US			Japan			The US			Japan			The US			Japan		
	All	Non-STEM	STEM	All	Non-STEM	STEM	All	Non-STEM	STEM	All	Non-STEM	STEM	All	Non-STEM	STEM	All	Non-STEM	STEM
Number of respondents	300	133	154	300	193	102	300	133	154	300	193	102	300	133	154	300	193	102
cybersecurity management	51%	45%	56%	32%	31%	35%	47%	38%	56%	30%	32%	28%	36%	81%	29%	26%	26%	25%
cybersecurity audit	27%	30%	24%	23%	20%	28%	37%	29%	44%	24%	21%	29%	26%	59%	21%	17%	15%	23%
Risk management	35%	35%	32%	18%	18%	18%	46%	47%	45%	18%	19%	16%	35%	80%	28%	17%	16%	19%
cybersecurity governance	30%	28%	31%	18%	17%	21%	47%	46%	49%	19%	19%	20%	31%	69%	24%	16%	17%	16%
Digital systems/business strategy/planning/procurement	27%	25%	29%	15%	12%	22%	40%	38%	43%	19%	14%	28%	26%	59%	19%	16%	14%	22%
System architecture	24%	24%	23%	12%	7%	21%	33%	24%	42%	13%	8%	24%	30%	68%	25%	10%	7%	17%
Digital product development	22%	20%	25%	11%	9%	16%	32%	25%	39%	11%	8%	17%	31%	69%	19%	12%	11%	15%
Digital product operation, vulnerability diagnosis, penetration tests and cybersecurity monitoring	19%	17%	21%	12%	11%	15%	35%	29%	41%	13%	9%	21%	30%	68%	22%	13%	11%	18%
cybersecurity monitoring and operation	24%	22%	26%	12%	11%	15%	39%	32%	46%	16%	16%	16%	34%	77%	25%	15%	15%	15%
cybersecurity survey analysis and research and development	21%	23%	19%	9%	7%	13%	36%	30%	42%	10%	6%	17%	33%	74%	25%	11%	9%	15%
Other cybersecurity & privacy services	13%	13%	14%	18%	20%	15%	25%	29%	21%	27%	27%	25%	23%	51%	19%	15%	15%	17%
Operations other than cybersecurity privacy	22%	20%	23%	23%	24%	20%	0%	0%	0%	0%	0%	0%	18%	40%	21%	22%	23%	17%

In both the US and Japan, the percentage of cybersecurity professionals who were involved in cybersecurity business was approximately 80% in the previous job or department.

■ 80% or more ■ 70%~79% ■ 60%~69% ■ 50%~59% ■ 40%~49%
■ 30%～39% ■ 20%~29% □ 10%~19% ■ 0%~9%

Q. Tell us everything that applies to your current work tasks. Please also answer any questions about tasks you have previously managed or wish to manage in the future.

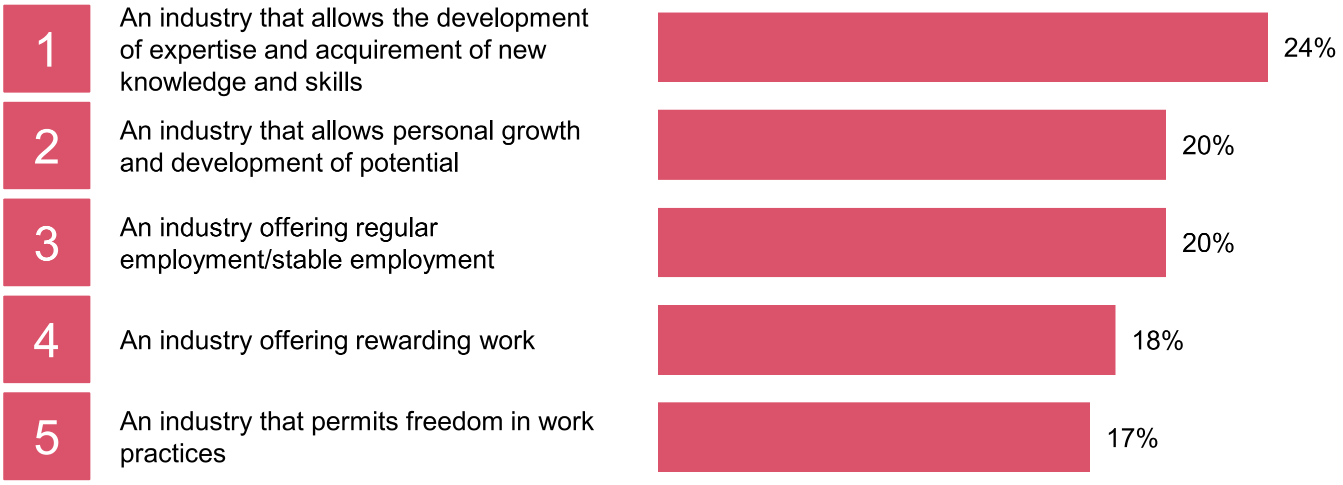
Many students and career changers coming from other industries or departments apparently believe that ‘the cybersecurity industry requires skills and experience in hacking techniques, coding and other engineering and technical areas’. However, as the data shows, there are also many tasks related to cybersecurity strategy, system development, regulation formulation, education and other governance-related tasks. There are also many survey-related tasks concerning geopolitical risks, regulatory compliance, open-source intelligence (OSINT)[3] and other matters that do not necessarily require engineering knowledge. Therefore, we hope people who are interested in the cybersecurity industry will feel comfortable taking on the challenge even if they lack experience in engineering.

[3] OSINT is one of the research methods of correcting and analyzing information on the web, including dark web.

(6) The top impressions after working in the cybersecurity industry: ‘An industry that allows the development of expertise’.

When we asked Japanese and US professionals (n=600) about their impressions of the cybersecurity industry after actually working in it, the top response was that it is ‘an industry that allows the development of expertise and acquirement of new knowledge and skills’ at 24%, followed by ‘an industry that allows personal growth and development of potential’ and ‘an industry offering regular employment/stable employment’ at 20% each, ‘an industry offering rewarding work’ at 18% and ‘an industry that permits freedom in work practices’ at 17% (Figure 12).

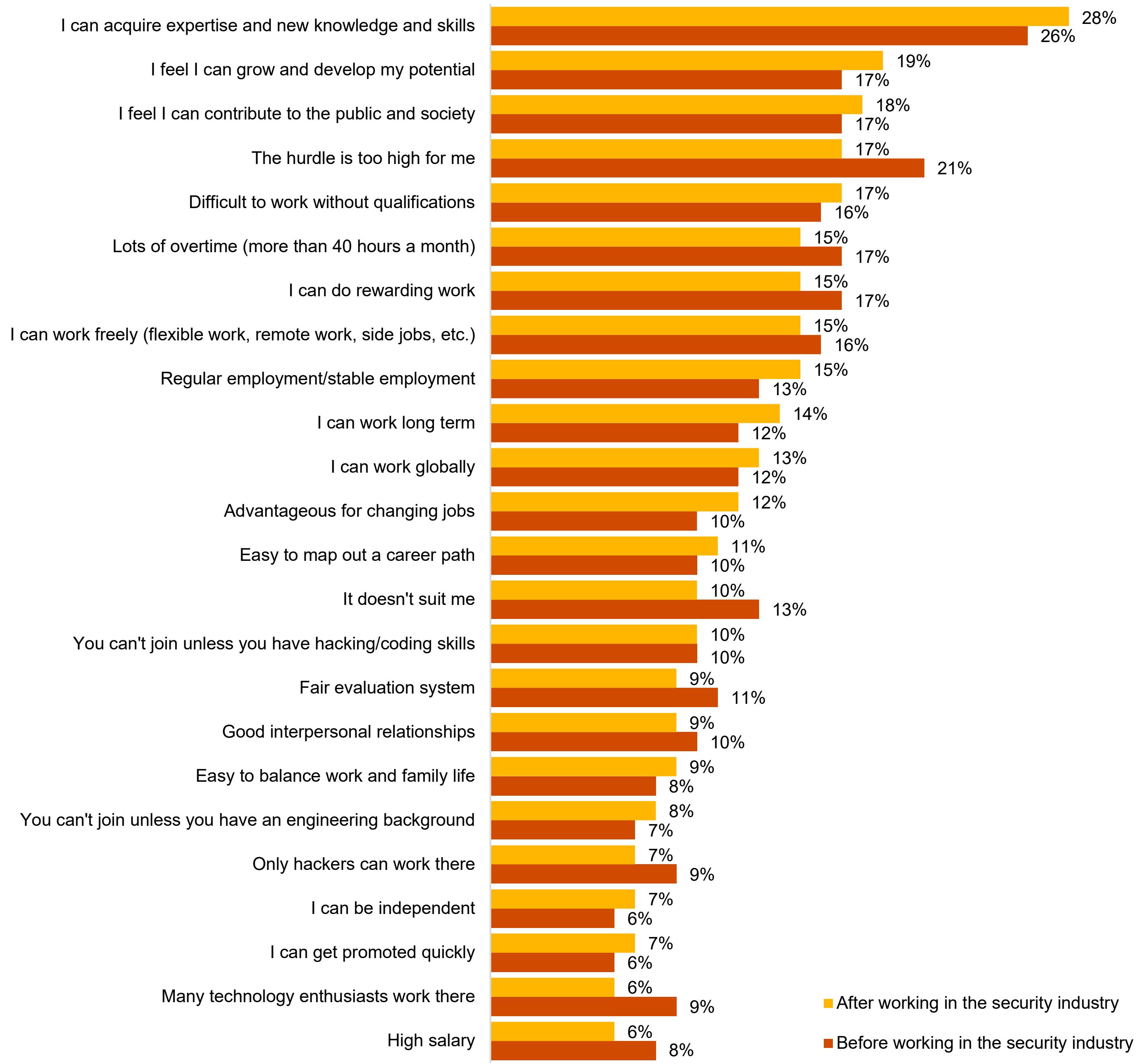
Figure 12: Impressions of the cybersecurity industry after working in it (top five impressions; n=600)



Q. Please tell us three impressions you have of cybersecurity and privacy work that apply to you, or impressions you currently have.

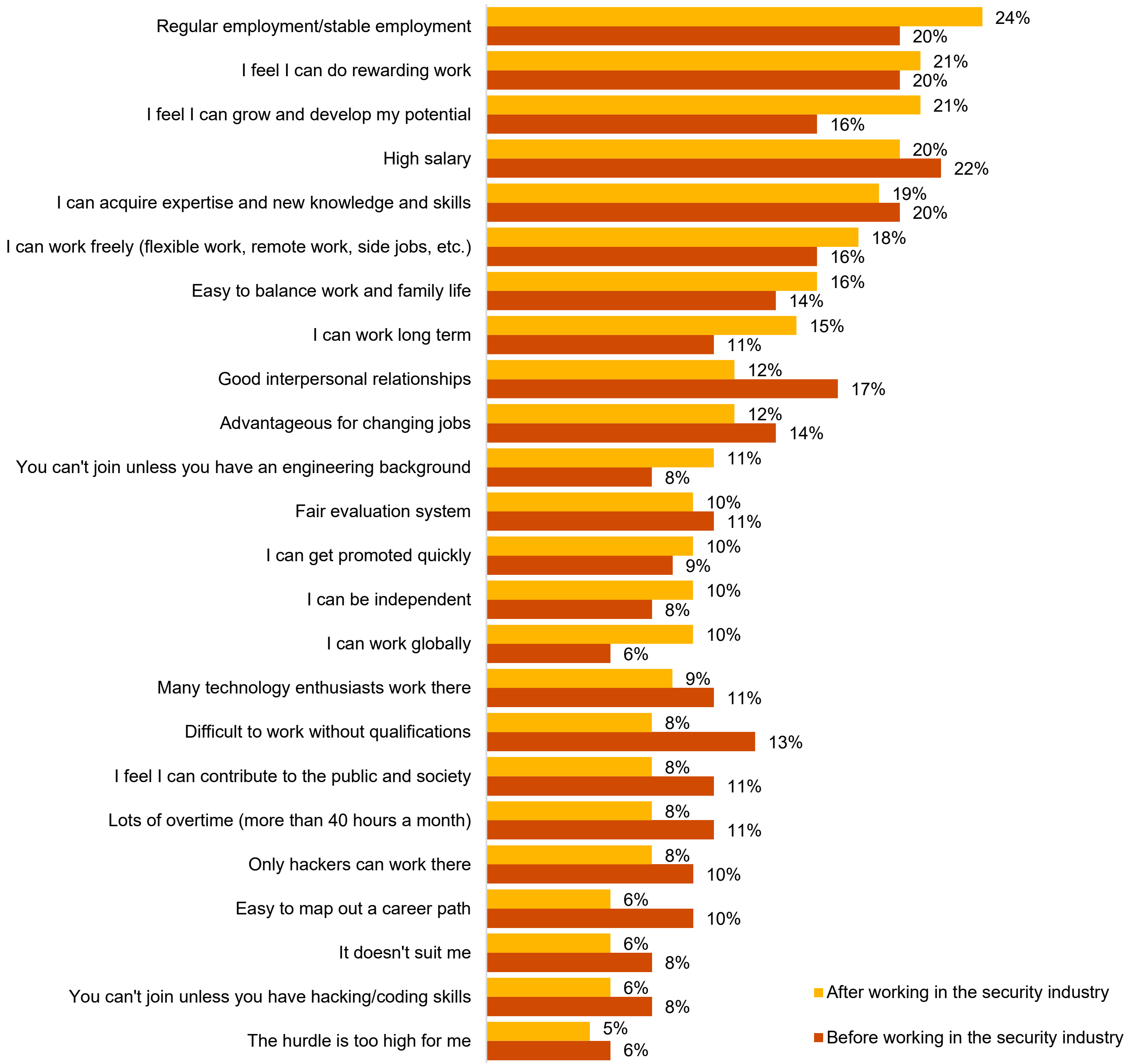
Looking at the top three impressions of working in the industry among Japanese professionals (n=300), at the top was ‘I can acquire expertise and new knowledge and skills’ at 28%, followed by ‘I feel I can grow and develop my potential’ at 19% and ‘I feel I can contribute to the public and society’ at 18% (Figure 13). As for the top three impressions of working in the industry among US professionals (n=300), at the top was ‘regular employment/stable employment’ at 24%, followed by ‘I feel I can grow and develop my potential’ and ‘I feel I can do rewarding work’ at 21% each (see Figure 14). For detailed data on the comparisons between male and female professionals in Japan and the US, please refer to Appendix Figure 39, Figure 40 and Figure 41.

Figure 13: Comparison of impressions of the cybersecurity industry before and after working in it (Japan)



Q. Please tell us three impressions you have of cybersecurity and privacy work that apply to you.

Figure 14: Comparison of impressions of the cybersecurity industry before and after working in it (US)

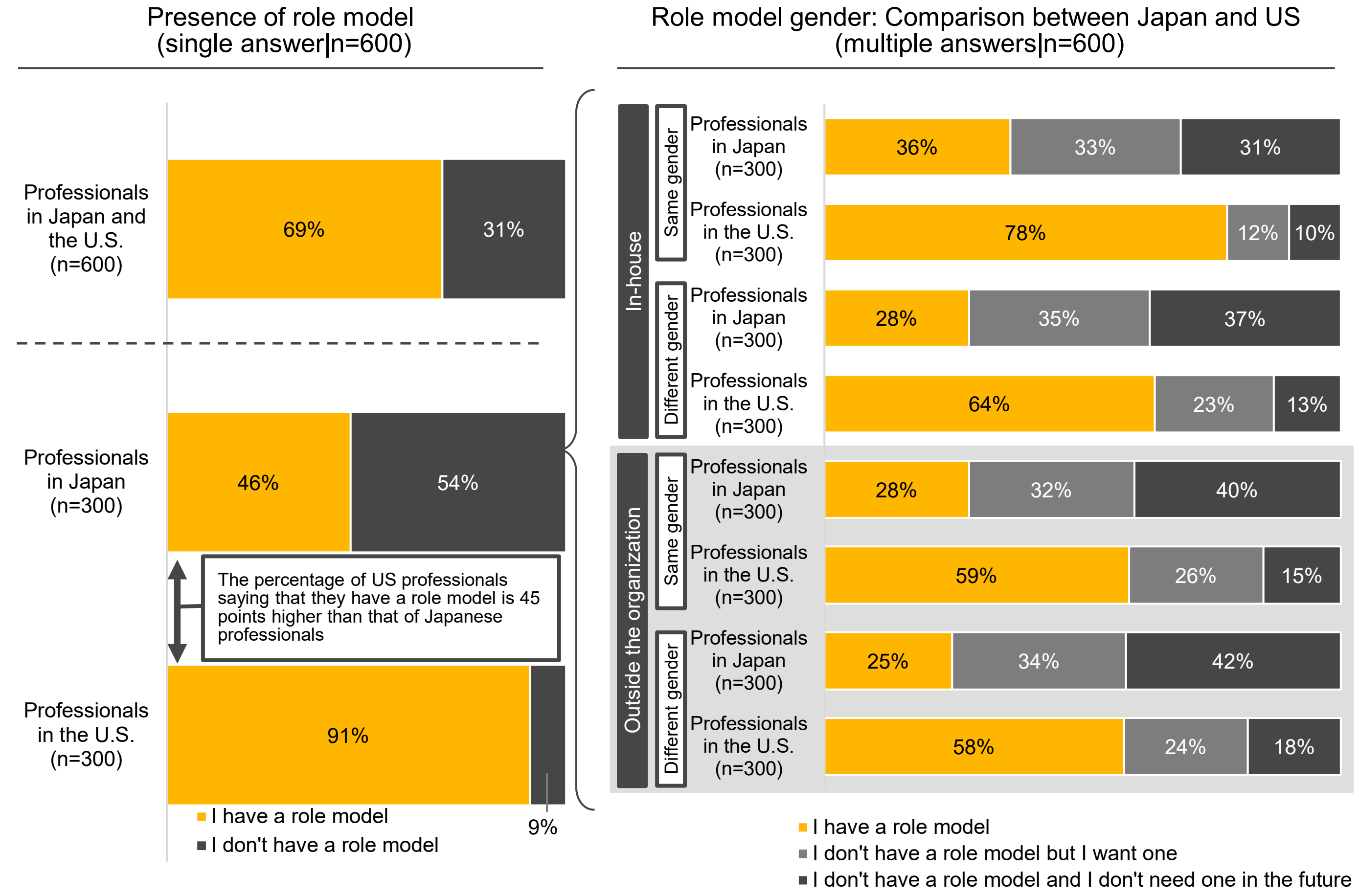


Q. Please tell us three impressions you have of cybersecurity and privacy work that apply to you.

(7) Seventy percent of Japanese and US professionals have role models. Many of them rated their work satisfaction positively, saying they are ‘satisfied with cybersecurity work’.

When we next asked respondents about their ‘work satisfaction’, we found that, for both Japanese and US professionals, work satisfaction was conspicuously higher in the group that had role models (n=415) than the group that did not (n=185) (Figure 15 and Figure 16).

Figure 15: ‘Presence/absence of a role model’ among Japanese and US professionals

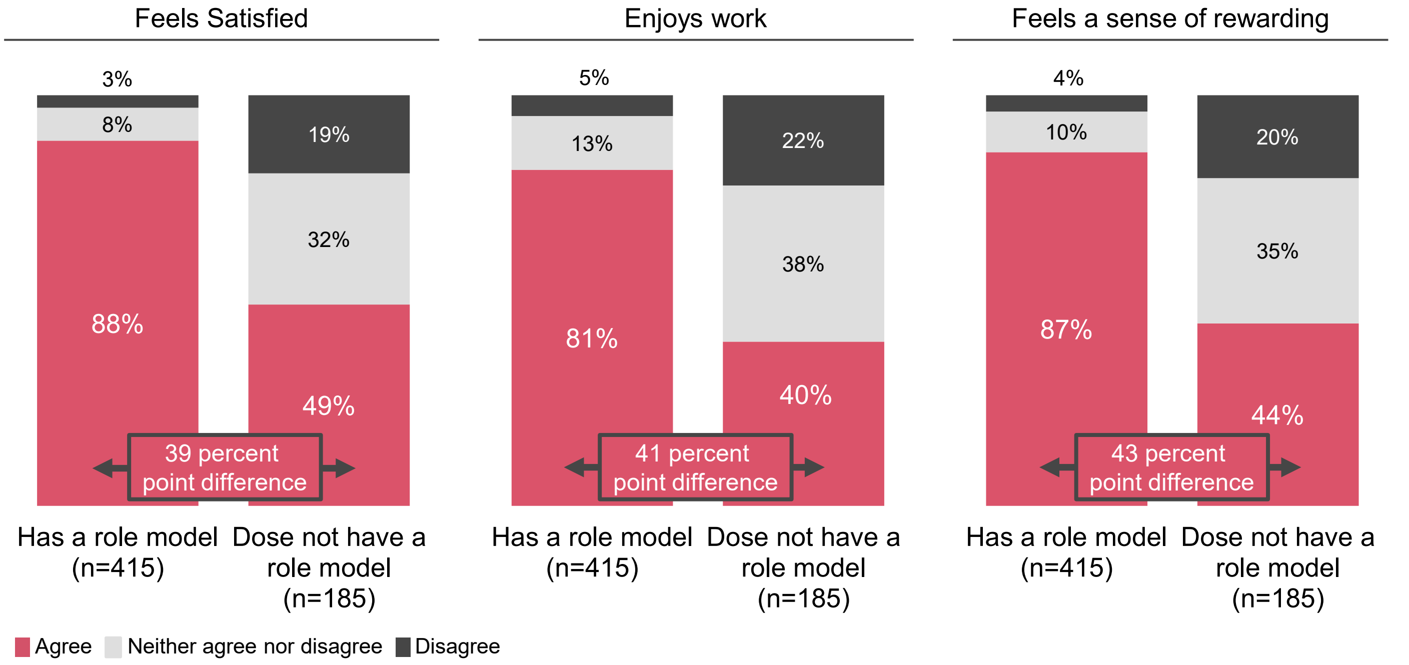


Q. When working in the cybersecurity privacy industry, do you have a role model (a person or ideal that serves as an example) to guide you in designing your career path?

When we then asked respondents if they are ‘satisfied (enjoy/fulfilled)’ by their cybersecurity work, the data showed that the group that ‘has a role model’ (n=415) had a high rate of work satisfaction at over 80% (see Figure 16).

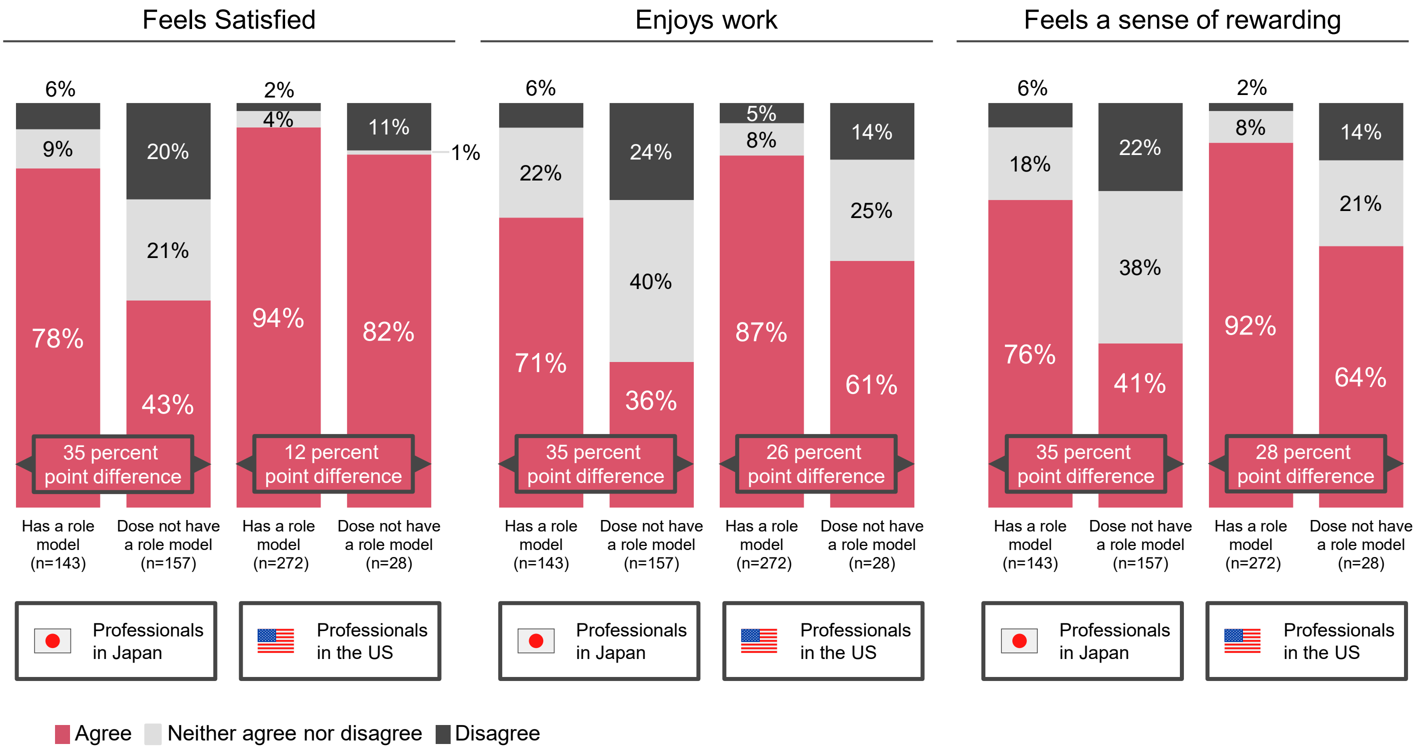
This trend is evident in both Japan and the US (Figure 17), suggesting that finding a personal role model is useful for experiencing fulfilment and enjoyment when working in the cybersecurity industry.

Figure 16: Satisfaction (enjoyment, feeling of fulfilment) in your cybersecurity work (comparison of role model/no role model)



Q. Are you satisfied with your current job? Or Do you find it fun or rewarding?

Figure 17: Satisfaction (enjoyment, feeling of fulfilment) in your cybersecurity work (comparison of role model/no role model between Japan and the US)



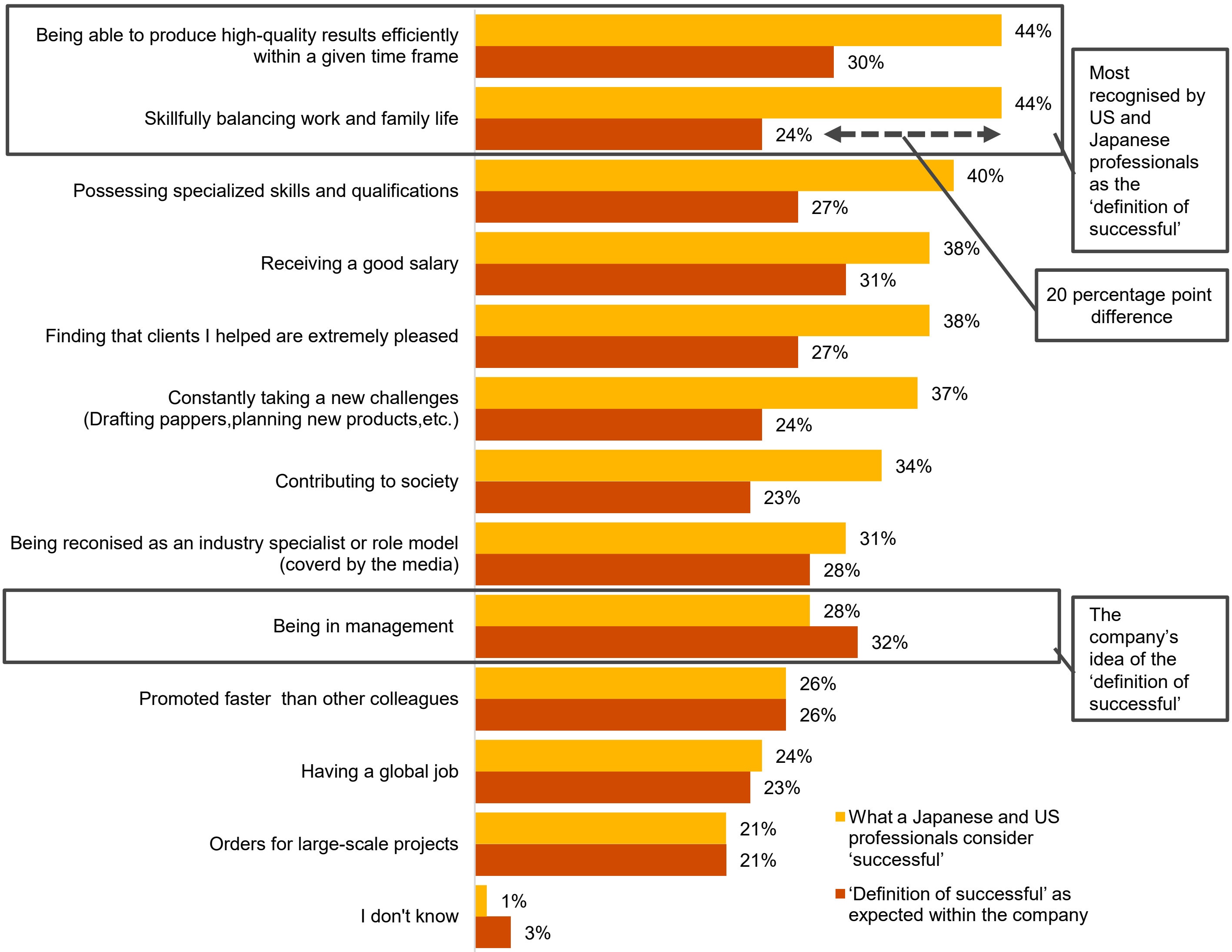
Q. Are you satisfied with your current job? Or Do you find it fun or rewarding?

(8) The top ‘definition of successful’ as considered by professionals is ‘being able to produce high-quality results efficiently within a given time frame’. However, there is a divergence with the top definition as expected within the company, which is ‘being in management’.

Often, ‘successful’ is defined in Japan as ‘being in management’ (or at the executive level). However, what do Japanese and US professionals actually consider ‘successful’ to mean? In this year’s survey, we asked respondents for their ‘definition of successful’ from their standpoint as professionals. In addition, we asked about their ‘definition of successful’ as expected within the company, and we found a divergence between the two definitions (Figure 18).

When we asked Japanese and US professionals (n=600) to indicate their ‘definition of successful’, the most common responses were ‘being able to produce high-quality results efficiently within a given time frame’ and ‘skilfully balancing work and family life’ at 44% each, followed by ‘possessing specialised skills and qualifications’ at 40% and ‘finding that clients I helped are extremely pleased’ and ‘receiving a good salary’ at 38% each. On the other hand, ‘being in management’, which was selected most frequently as the ‘definition of successful’ from the company’s standpoint, tended to be less important.

Figure 18: Comparison of ‘definition of successful’ as considered by Japanese and US professionals and ‘definition of successful’ as considered within the company (multiple responses accepted; n=600)



Q. What exactly do you think are the terms for you to be active in your work? Also, please tell us all the things that apply to you, including the characteristics of people who are highly regarded in your company.

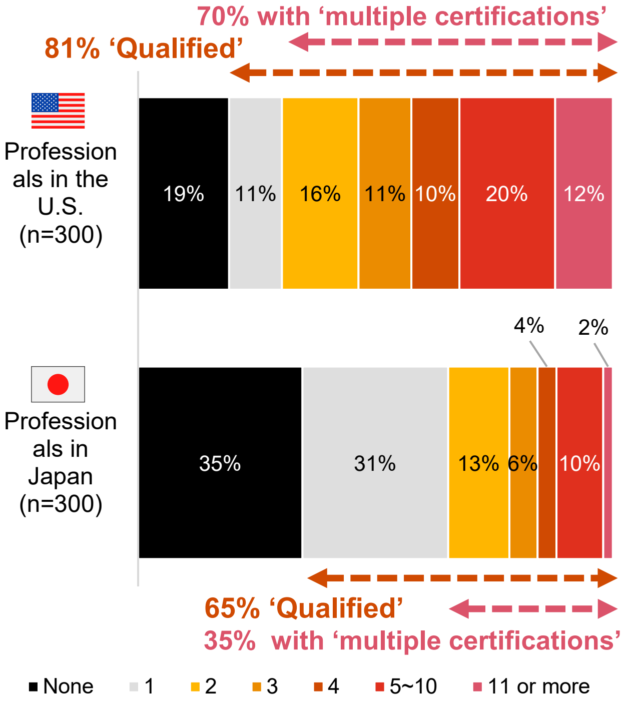
(9) ‘Cloud security-related certification’ stands at the top of certifications ‘most useful for work’.

Next, we examine how many Japanese and US professionals have cybersecurity-related certifications and their ‘usefulness’.

Looking at the status of certification among Japanese and US professionals, we found that 81% of US professionals have a certification, which is 16 percentage points higher than the 65% of Japanese professionals who have a certification. Moreover, US professionals tended to have multiple certifications, with those with multiple certifications accounting for 70% of the total. This figure is high compared to 35% of Japanese professionals (Figure 19, left). The specific certifications are shown in Figure 19 (right).

Figure 19: Status of cybersecurity-related certifications among Japanese and US professionals

Percentage of cybersecurity-related certifications
(Japan-US comparison|n=600)



More than 80% of US professionals are certified and are 16 points higher than Japanese professionals. In addition, 70% have multiple certifications, which is 35 points higher than that of Japanese professionals.

Comparison of the top 10 certifications in Japan and the US
(Japan-US comparison|n=420)

Qualified US professionals (n=223)

1	AWS Certified Security – Specialty	42 %
2	Certified Cloud Security Professional（CCSP）	38 %
3	Certified Information Privacy Manager（CIPM）	31 %
3	Certified Information Security Manager（CISM）	31 %
5	Certified Information Privacy Professional（CIPP）(iapp)	29 %
6	Certified Information Systems Security Professional（CISSP）	27 %
6	Certified Data Privacy Solutions Engineer	27 %
8	Certified Ethical Hacker（CEH）	25 %
9	Certified in Risk and Information Systems Control（CRISC）	22 %
10	Project Management Professional（PMP）	21 %

Qualified Japanese professionals (n=197)

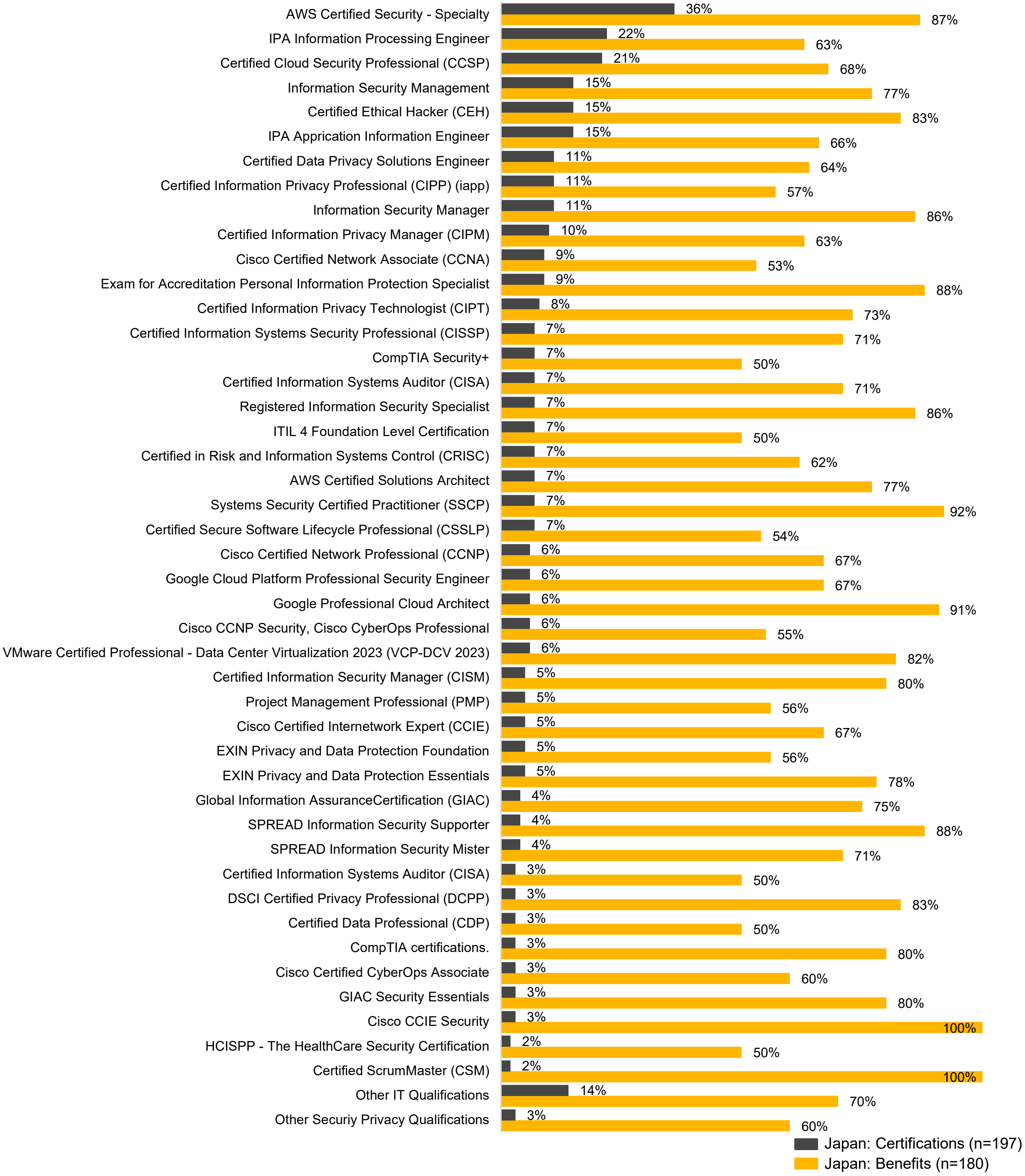
1	AWS Certified Security – Specialty	36 %
2	IPA Information Processing Engineer	22 %
3	Certified Cloud Security Professional（CCSP）	21 %
4	Information Security Management	15 %
4	Certified Ethical Hacker（CEH）	15 %
4	IPA Application Information Engineer	15 %
7	Certified Data Privacy Solutions Engineer	14 %
8	Information Security Manager	11 %
8	Certified Information Privacy Professional（CIPP）(iapp)	11 %
8	Certified Information Privacy Manager（CIPM）	11 %

🟨 Certifications that are in the top 10s of both US and Japanese professionals

Q. What certifications do you have in relation to cybersecurity privacy practices?

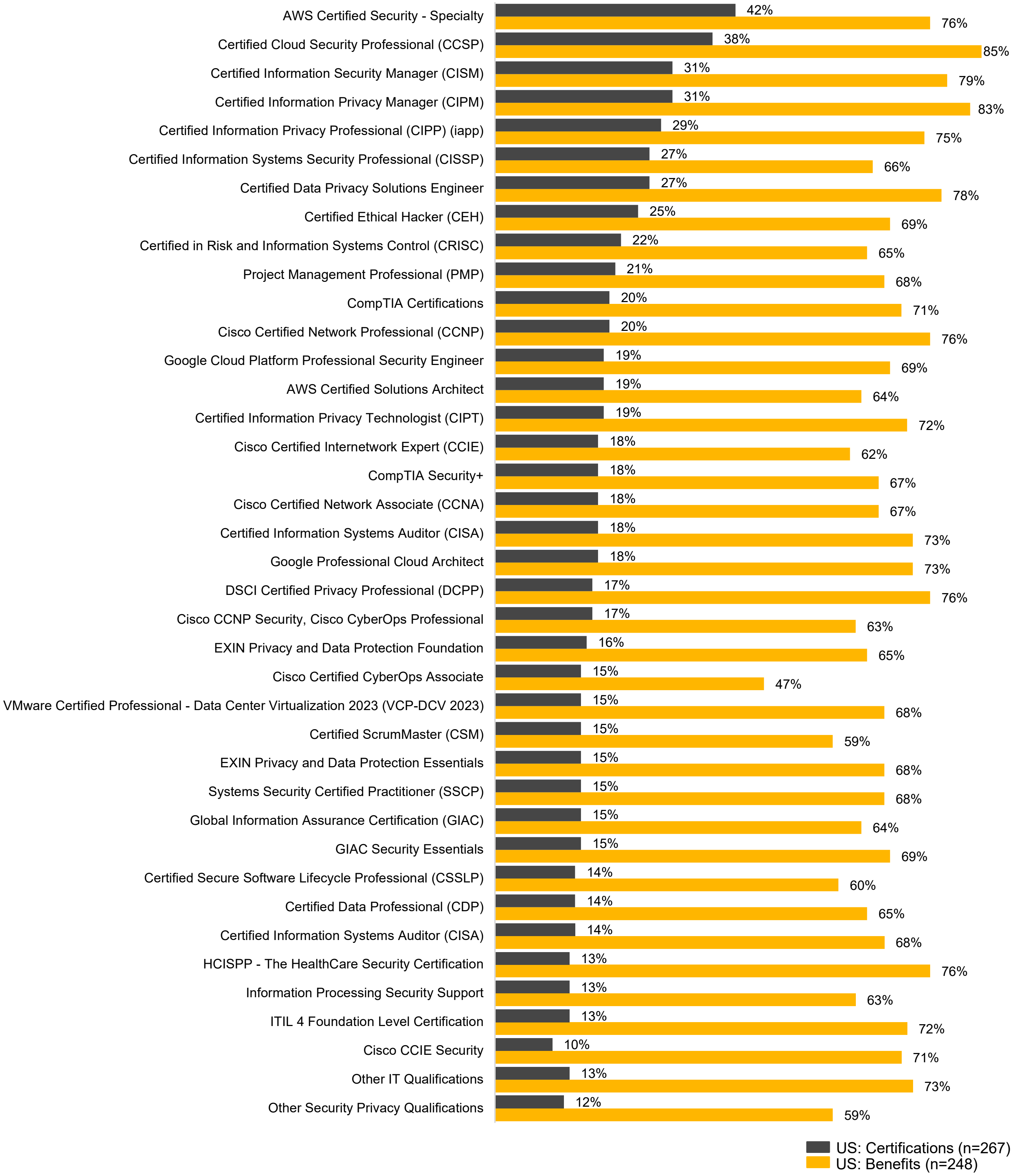
When we asked the respondents whether the certifications they obtained were useful for their work, for almost all of the certifications mentioned, more than half of both Japanese and US professionals felt that the certification was useful. See Figure 20 and Figure 21 for details.

Figure 20: Certifications held by Japanese and US professionals and their usefulness (Japan)



Q. What certifications do you have in relation to cybersecurity privacy practices? Also, please tell us about any of them that were beneficial to your business.

Figure 21: Certifications held by Japanese and US professionals and their usefulness (US)

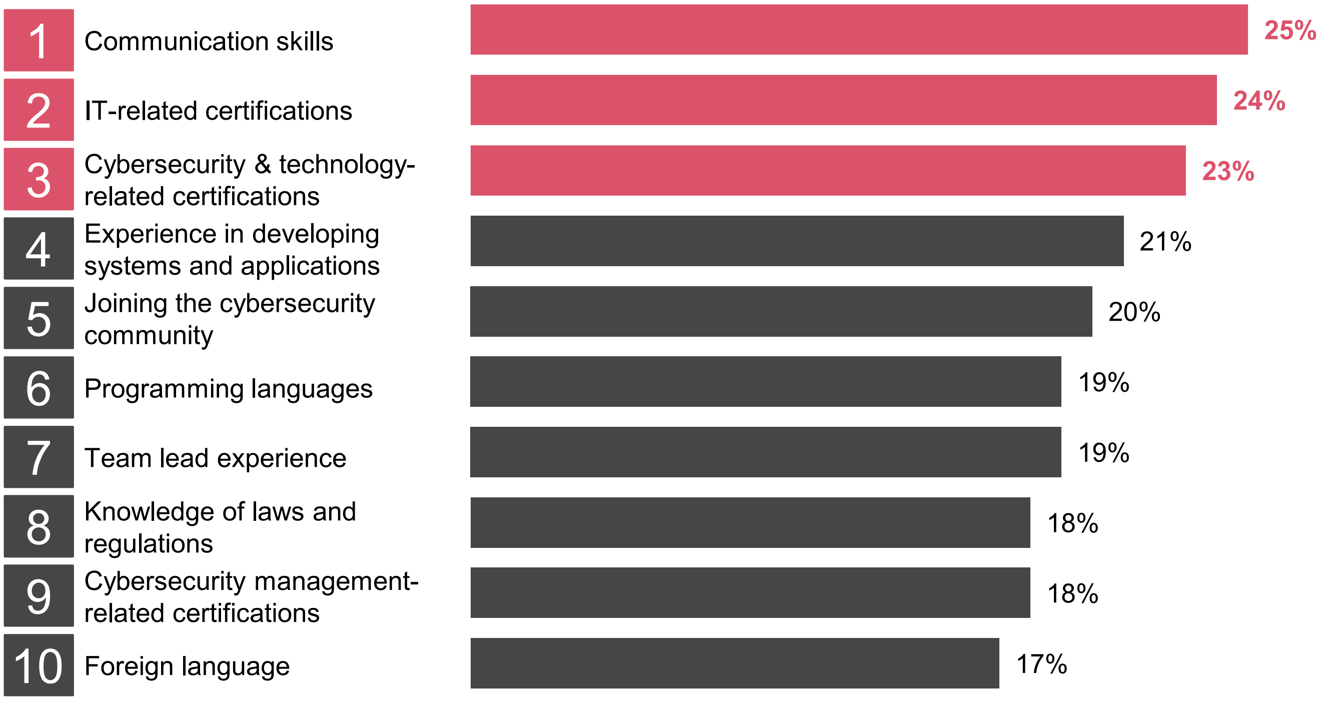


Q. What certifications do you have in relation to cybersecurity privacy practices? Also, please tell us about any of them that were beneficial to your business.

(Reference) Skills and experience recommended by Japanese and US professionals

Through the survey, we found that Japanese and US professionals recommended ‘communication skills’, ‘IT-related certifications’ and ‘cybersecurity technology-related certifications’ as skills and experience that future students and career changers desiring to work in the cybersecurity industry should acquire (Figure 22). We hope these findings will be useful for people wanting to pursue a career in the cybersecurity industry.

Figure 22: Skills and experience that Japanese and US professionals recommend students and career changers should acquire before working in the cybersecurity industry (top 10 responses; n=523)



Q. Please tell us all the skills and experiences that you recommend to students and career changers who want to become future cybersecurity professionals that you think would be advantageous to study and experience beforehand.

Future trends

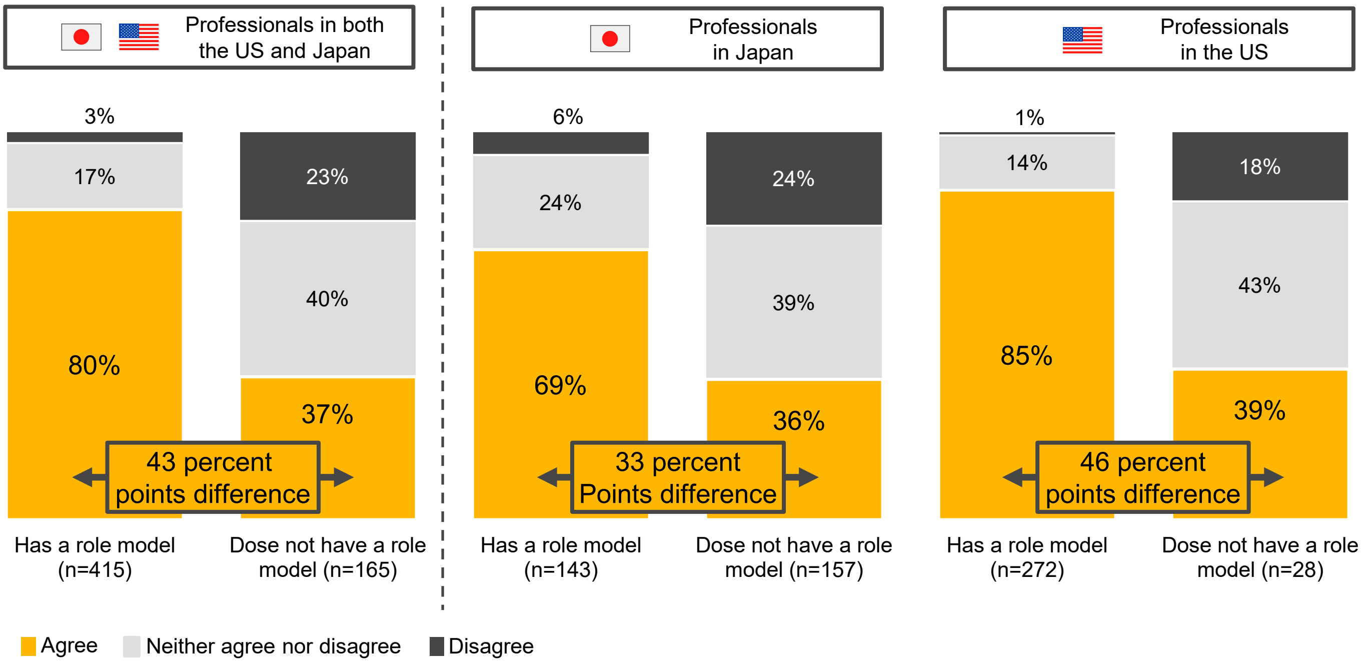
In this chapter, we will look at how Japanese and US professionals see their career paths taking shape in the future.

(10) Eighty percent of Japanese and US professionals with role models 'want to work in the cybersecurity industry for a long time'.

The most notable future trend is that 80% of the 'has a role model' group answered that they 'want to work in the cybersecurity industry for a long time'. This group was higher than the 'does not have a role model' group (less than 40% for each response category) (Figure 23).

Thus,it could be argued that, when charting a career path in the cybersecurity industry, finding a personal role model to emulate can lead to a long and fulfilling career in the cybersecurity industry.

Figure 23: Percentages of respondents who want to work in the cybersecurity industry for a long time (presence/absence of a role model, Japan-US comparison)



Q. Do you want to work in the cybersecurity industry for a long time?

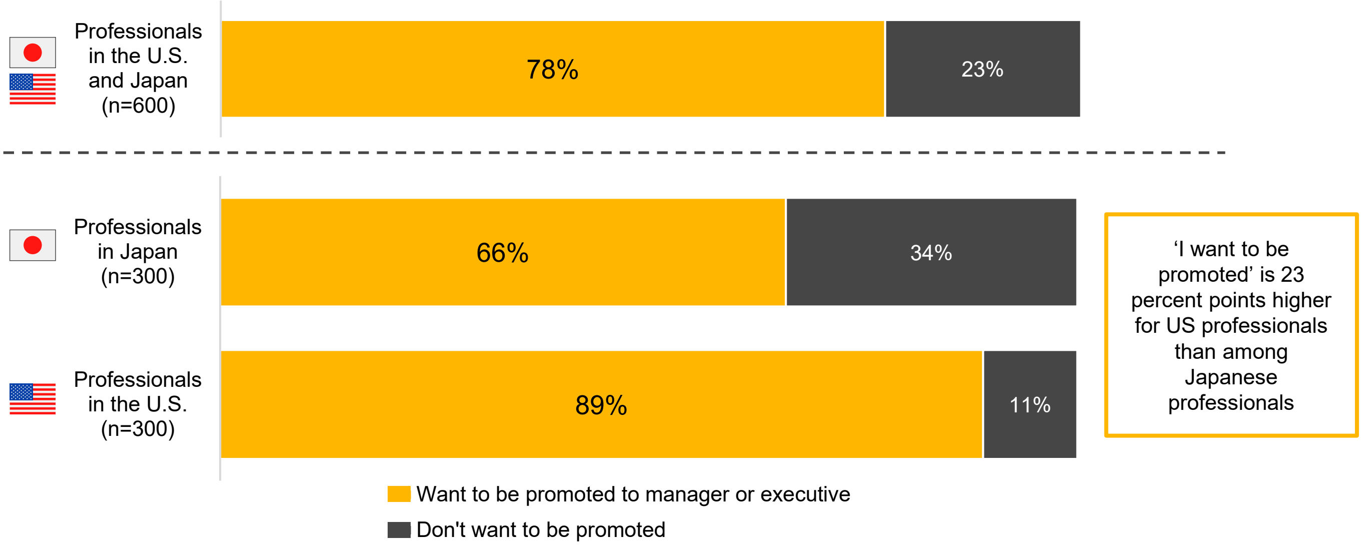
(11) Most US professionals (more than 80%) want to be promoted. This number is higher than that of Japanese professionals.

Next, let's look at the future intentions of Japanese and US professionals in terms of 'promotions', 'desired area of work (specialist/generalist)' and 'career change'.

■ Desire for promotion

When we asked Japanese and US professionals about their desire to be promoted to management or an executive-level position (or desire to continue at the same level), 90% of US professionals responded that they 'want to be promoted'. This was higher than the 70% of Japanese professionals (Figure 24). *See Appendix Figures 42 and 43 for reasons for wanting a promotion.

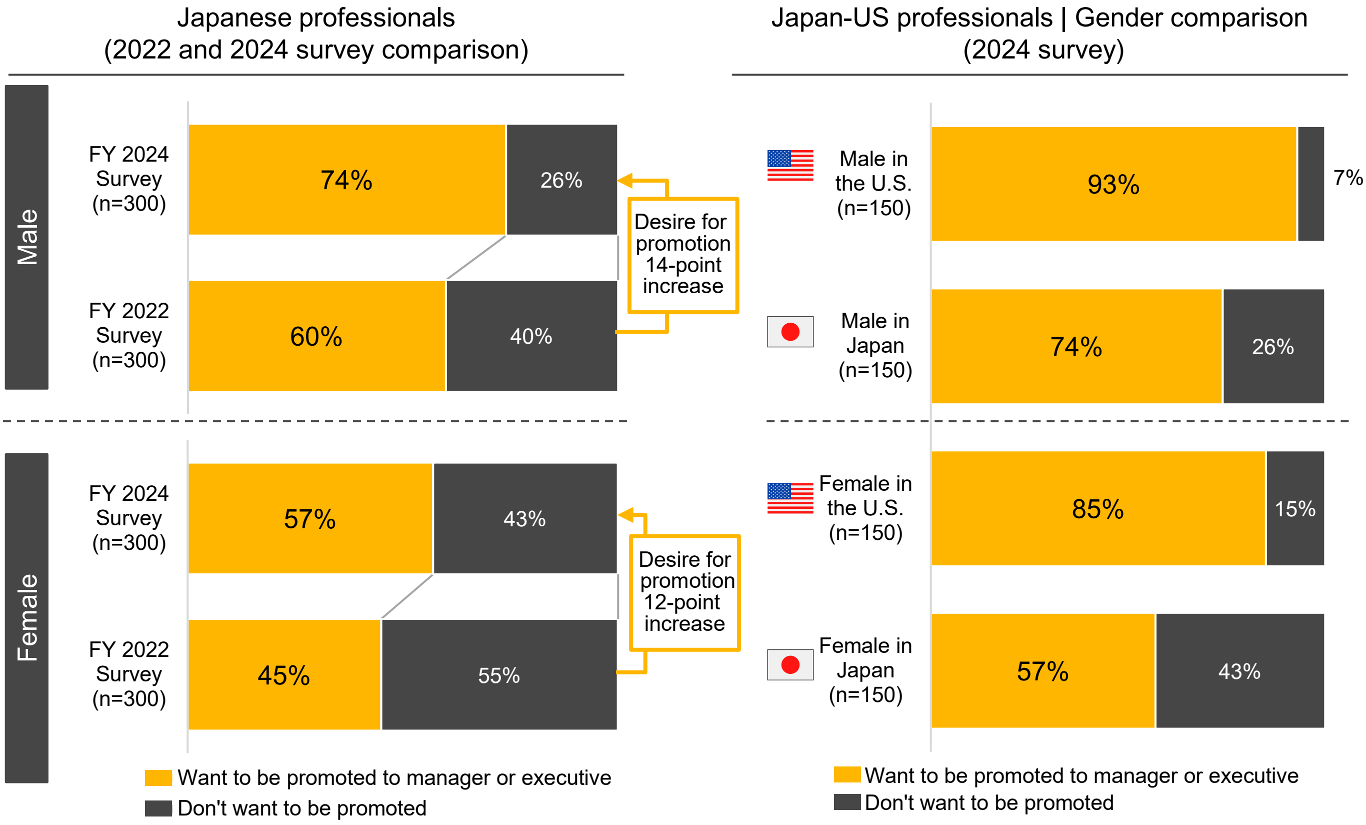
Figure 24: Desire to be promoted to management or executive-level position (Japan-US comparison)



'I want to be promoted' is 23 percent points higher for US professionals than among Japanese professionals

Q. Do you want to take the next step in your career and become a manager or executive?
If you are currently in a managerial position or above, do you want to continue in that position?

Figure 25: Desire to be promoted to management or executive-level position (gender comparison)

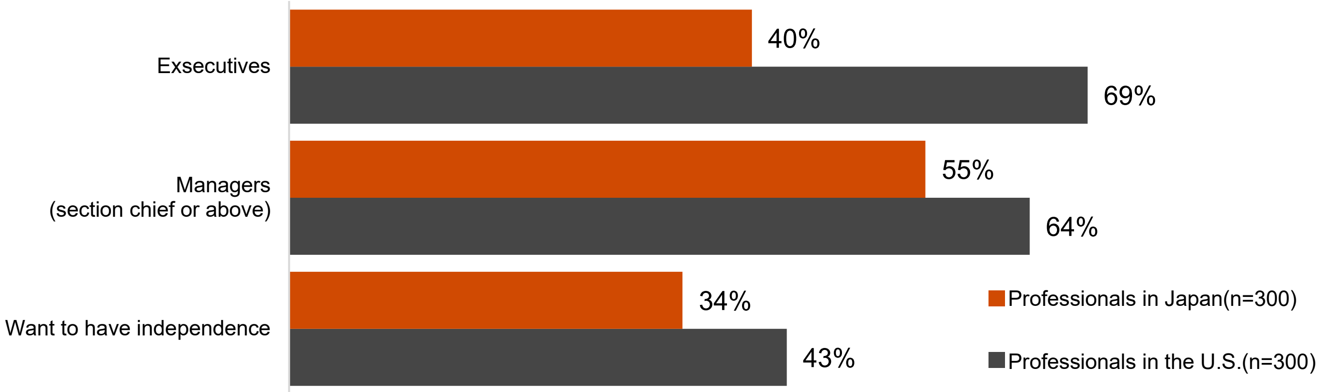


Q. Do you want to take the next step in your career and become a manager or executive?
If you are currently in a managerial position or above, do you want to continue in that position?

Desire for independence

Furthermore, an analysis of respondents' desire for independence shows that 43% of US professionals answered that they want to be independent, while 34% of Japanese professionals gave the same answer. No particular gender difference was observed in either country (Figure 26).

Figure 26: Desire for promotion and desire for independence



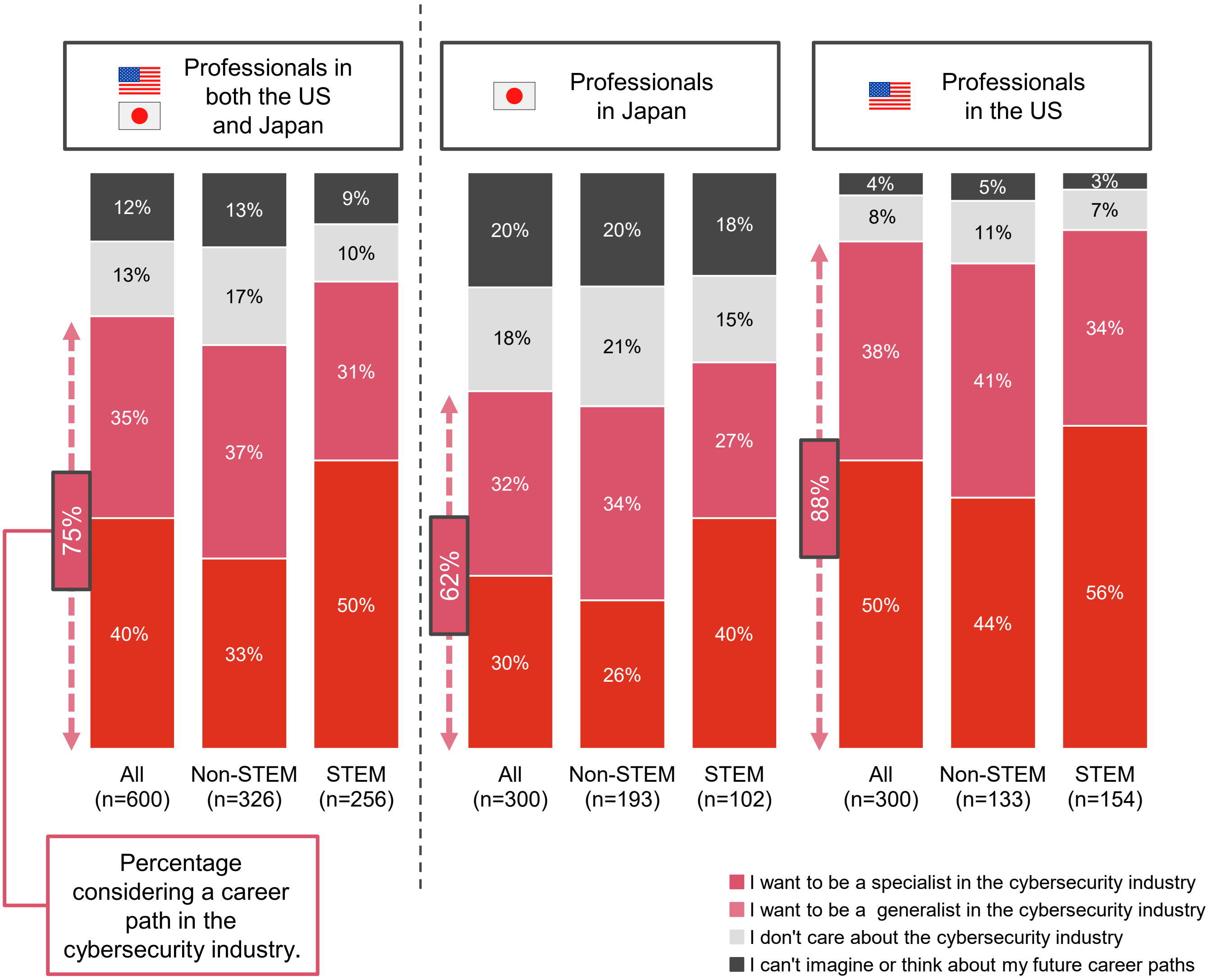
Q. for your next career step, would you like to become a manager or executive, or be independent?

Desire to become a ‘specialist’ or ‘generalist’

When we asked Japanese and US professionals whether they are considering a career path in the cybersecurity industry, a majority (75%) responded that they were ‘considering a career path in the cybersecurity industry’. Of these, 40% said they were aiming to become ‘specialists’ and 35% were aiming to become ‘generalists’ (Figure 27).

A comparison between the group with STEM backgrounds and the group with non-STEM backgrounds reveals that a large percentage of professionals with STEM backgrounds (n=256)—about half of the total—were aiming to become ‘specialists in the cybersecurity industry’. This percentage was 17 percentage points higher than the 33% of professionals with non-STEM backgrounds (n=326).

Figure 27: Future intentions of Japanese and US professionals: Specialist/generalist

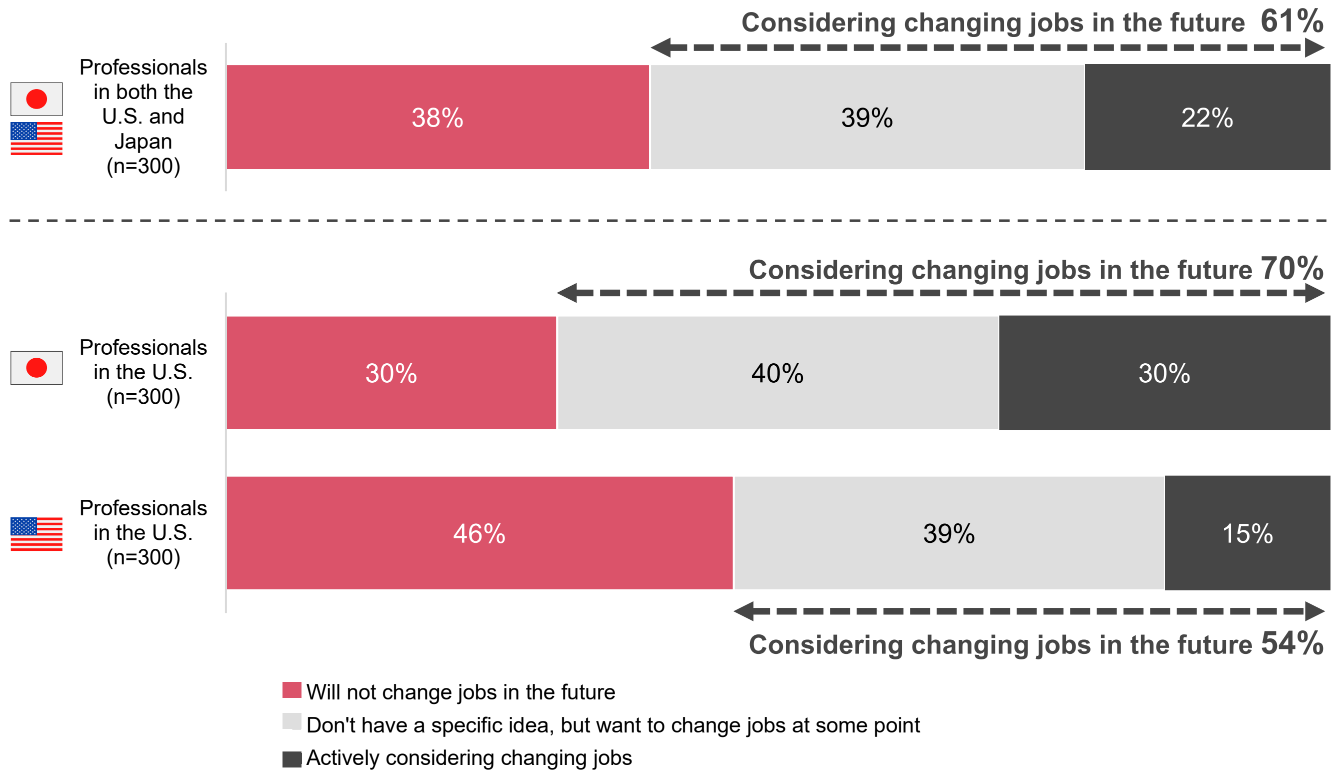


Q. Which best fits your intentions for your future career path working in the cybersecurity industry?

■Desire for career change

Next, when we asked Japanese and US professionals about their intention to change careers, 60% responded that they were ‘considering changing jobs in the future’. This trend was somewhat stronger among Japanese professionals (70%) than among US professionals (50%) (Figure 28). *Refer to Appendix Figure 47 for past ‘reasons for career change’ and future ‘reasons for wanting a career change’.

Figure 28: Status of considering future career change (Japan-US comparison)



Q. Please let us know your intentions regarding changing jobs.

(12) Experience in ‘IT and cybersecurity practice’ and ‘consulting’ is the most beneficial for a person wishing to become a cybersecurity-related CxO [Chief x Officer].

It is clear from the survey that Japanese and US professionals believe that experience in ‘IT and cybersecurity practice’ and ‘cybersecurity-related consulting’ are the most beneficial for a person desiring to reach the CxO level in the future (Figure 29).

Specifically, US professionals indicated that the experience most beneficial to someone aiming to become a Chief Information Security Officer (CISO) is ‘IT and cybersecurity practice’ at 66% (Japan: 32%), followed by ‘consulting (including cybersecurity governance and engineering)’ at 39% (Japan: 31%) and ‘compliance and legal affairs’ at 37% (Japan: 25%). As for experience beneficial to becoming a Chief Risk Officer (CRO), the most common response was ‘consulting’ at 47% (Japan: 38%), followed by ‘compliance and legal affairs’ at 46% (Japan: 27%) and ‘IT and cybersecurity practice’ at 37% (Japan: 24%). For Chief Data Officer/Chief Privacy Officer (CDO/CPO), the most common response was ‘consulting’ at 55% (Japan: 39%), followed by ‘IT and cybersecurity practice’ at 40% (Japan: 22%) and ‘compliance and legal affairs’ at 34% (Japan: 24%).

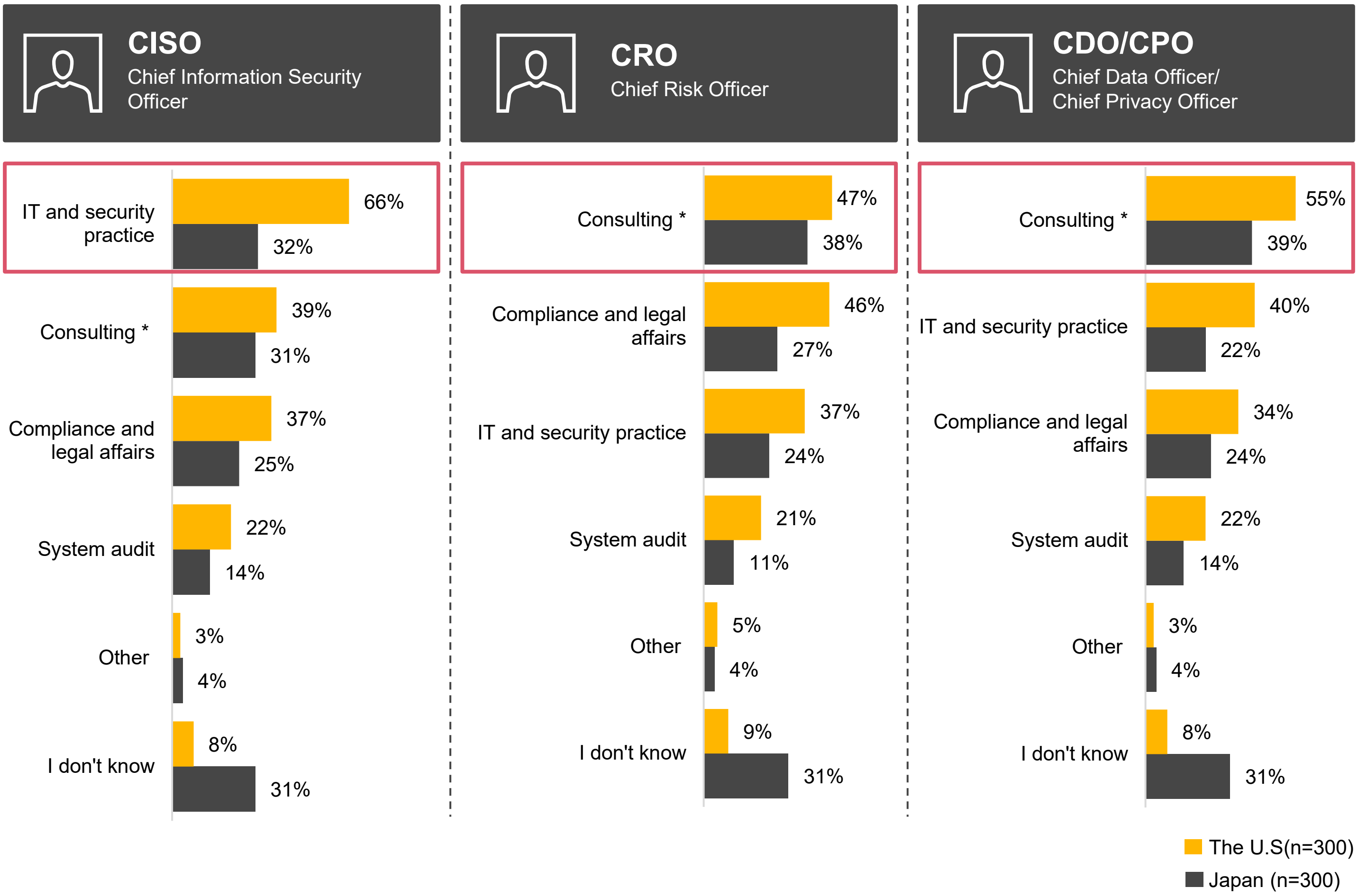
We surmise that a factor behind many US professionals’ selection of ‘IT and cybersecurity practice’, particularly for CISO, is that it is difficult to take responsibility, issue instructions and make decisions without practical experience. Another factor is that, in addition to there being many CISO career models available, the career model for becoming a CISO is relatively mature, particularly in listed companies, as US investors tend to prefer CISOs with practical experience .

On the other hand, a large percentage of Japanese professionals (around 30%) chose ‘I don’t know’, suggesting that it is difficult to get a clear picture of what a career path to CISO looks like. However, it is probable that a career model similar to that of the US, a leader in the cybersecurity industry, will be established in Japan in the future.

In light of these trends, those who are seeking CISO, CRO or CDO/CPO positions but have no experience in ‘IT and cybersecurity practice’ or ‘consulting’ work may want to consider gaining work experience in these areas as part of their next career path.

4. PwC「サイバーセキュリティおよびプライバシー情報開示」に関する日米投資家の意識調査2024」
https://www.pwc.com/jp/ja/knowledge/thoughtleadership/digital-trust-investor-survey2024.html

Figure 29: Areas of ‘cybersecurity work experience’ that Japanese and US cybersecurity professionals believe are beneficial for people aspiring to be a CISO, CRO or CDO/CPO



* Consulting here includes cybersecurity governance and engineering.

Q. Do you think that you have the necessary business experience to work as a cybersecurity professional in roles like CISO, CRO, CDO, etc.? Please provide details applicable to each role.

3. Messages for students and job seekers aiming to enter the cybersecurity industry in the future

3. Messages for students and job seekers aiming to enter the cybersecurity industry in the future

Please take a look at these messages from Sean King and Keiko Hayashi, Inclusion and Diversity (I&D) leaders at PwC Consulting LLC (here in after referred to as ‘PwC Consulting’), and Yasuji Ayabe, an Inclusion and Diversity (I&D) leader at PricewaterhouseCoopers Japan LLC.

Messages from the cybersecurity leader at PwC’s Inclusion and Diversity (I&D)

Please take a look at these messages from Sean King and Keiko Hayashi, Inclusion and Diversity (I&D) leaders at PwC Consulting LLC (here in after referred to as ‘PwC Consulting’), and Yasuji Ayabe, an Inclusion and Diversity (I&D) leader at PricewaterhouseCoopers Japan LLC.

“A dynamic and enriching career in cybersecurity

PwC Consulting Security and Privacy, I&D Lead Partner
Sean King

The growing need for cybersecurity professionals continues to be a huge issue. By some estimates there are more than 3.5 million cybersecurity jobs unfilled. The field continues to be dominated by males. Currently women make up only about 25% of the cybersecurity workforce globally. There is a huge opportunity to bridge the talent gap by involving more women in the arena of cybersecurity.

Oddly enough, there is still a stigma with cybersecurity. The media continues to perpetuate stereotypes that represent the industry as one consisting of only techies and mysterious ex-hackers. However, this is a pretty narrow and antiquated view of an extremely diverse profession.

Cybersecurity is a great option for women seeking a new career. It’s a rich domain which encompasses strategy, compliance, risk management, governance, people, and process, as well as data and technology. What’s more, cyber is very dynamic and closely aligned with current events and the geopolitical landscape. The broad range of knowledge, skills, and exposure you will gain through a cybersecurity career can take you very far. We encourage you to have a look.

[6] Cybersecurity Ventures, “Cybercrime Magazine: Cybersecurity Jobs Report: 3.5 Million Unfilled Positions In 2025" (2023/4/14）https://cybersecurityventures.com/jobs/

[7] ISC2, “Women in Cybersecurity: Women in the Profession” https://www.isc2.org/Insights/2024/04/Women-in-Cybersecurity-Report-Women-in-the-Profession

Activity as a ‘cybersecurity professional’ expected by society

Taiji Ayabe (I&D Lead Partner, PricewaterhouseCoopers Japan LLC)

What is your impression of working in the cybersecurity industry? Do you picture a special job done by people with special skills? Yes, it is a job done by experts, but there are many different fields of cybersecurity, and each has its own specialists. There are fields such as engineers who are authorities in cybersecurity technology, specialists in cyber risk visualisation, and experts in governance that establish the rules and governance necessary to realise risk management. There are also fields where diverse backgrounds are more active.

On the other hand, from a business perspective, our operations are continuously digitised, and cybersecurity is an essential area for carrying out our business operations safely and securely. In addition to our business operations, our daily life is increasingly digitised, and we expect that our cybersecurity personnel will be able to play an active role throughout society.

However, in the area of cybersecurity, it has been a long time since it was said that there was a shortage of human resources, especially in Japan.

We hope that many people will become interested in the field of cybersecurity, which is vital to society and welcomes people from various backgrounds, and that you will become a cybersecurity expert.

Aiming to create a cybersecurity industry where diverse talent can participate with high aspirations

Keiko Hayashi (Senior Manager, I&D Lead, Trust Consulting Division, PwC Consulting Technology & Digital Consulting)

At PwC Consulting, an industry leader in cybersecurity and privacy, we are pleased to be able to make such announcements again.

Technology-driven innovation is being promoted daily in the cybersecurity industry, but people are the source of innovation. By promoting the attractiveness of careers in the cybersecurity industry, we hope to encourage more people to join this important field, both in Japan and globally.

In Japan, as someone who is still promoting I&D in the middle of the road, I would like to assist a diverse range of talents, regardless of career, gender or academic major, to actively participate in the cybersecurity industry and contribute to a more innovative society.

4. Conclusion

4. Conclusion

In this survey, the data show that the cybersecurity industry in the US and Japan, which are worldwide drivers of the industry, is one where people from both non-STEM and STEM backgrounds are actively involved. Approximately 80% of those with a role model also feel that their work is ‘rewarding’ and ‘enjoyable’, and that they want to work for a long time.

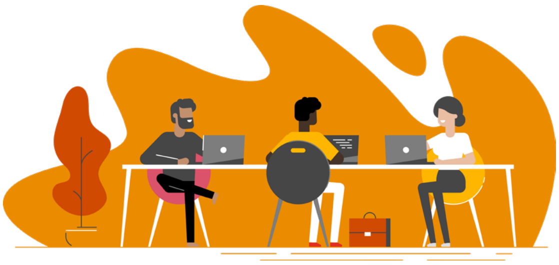
Unfortunately, in the cybersecurity industry, career paths and models are not as mature due to its shorter history compared to other industries. However, this can be seen as an industry where Japanese cybersecurity experts have the opportunity to create their own career models. I would be delighted if you would consider the cybersecurity industry as one of your employment opportunities.

To all students who are considering employment

In the cybersecurity industry, there are many students with backgrounds not only in science but also in the humanities. We hope that students majoring in the humanities will also consider the cybersecurity industry as one of their employment opportunities.
In PwC Japan study groups, specialists from various humanities-related backgrounds, primarily graduates in linguistics (foreign languages), international relations and legal-related departments, are actively engaged. The cybersecurity industry must respond to rapidly changing trends, such as cross-border cyberattacks and international laws and regulations on data. For this reason, there are numerous tasks that protect people and society from global threats posed by criminals.

As you can see from the survey results, those who want to ‘acquire expertise and new knowledge and skills’, ‘contribute to the public and society’ and have ‘regular and stable employment’ will be able to fulfil their wishes in the cybersecurity industry.

Do you want to be a cybersecurity specialist or privacy specialist? The cybersecurity industry itself has a short history, and through your dedication and hard work, you have the chance to become a leader in the field of cybersecurity.

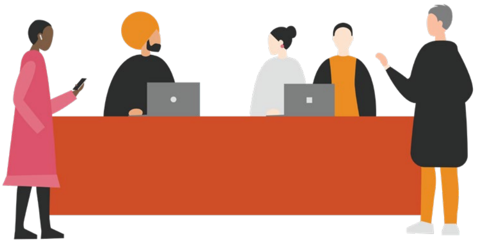


To anyone who is considering a job change or currently in the process of changing jobs

The cybersecurity industry in Japan has a high regular employment rate of over 90%[8]. It is considered an attractive industry for those changing jobs due to the perception of ‘acquiring specialised skills’ and being in ‘a seller’s market’. The survey also showed that most experts working in the cybersecurity industry are from non-IT departments, including those who have transitioned from sales, human resources, administration, etc. In fact, as mentioned in ‘Talents in Cyber Security and Privacy’ a number of specialists from non-IT departments, such as sales, marketing and legal, are also active in PwC Consulting. It can be said that both individuals currently active in the IT department and those in non-IT departments have a place in this industry.

Even without experience in the cybersecurity industry in particular, if you have expertise in areas such as ‘knowledge about experienced in the manufacturing’ or ‘knowledge about experienced in the finance industry’, you can specialise in ‘cybersecurity’ in those domains. This will allow you to develop your own area of expertise that others do not have.

Having ‘one’s own domain of expertise’ opens up a future where you can become a national pioneer and eventually a global pioneer. I wish you all the best in your endeavours.



[8] See Figure 35

5. Survey overview

5. Survey overview

Survey title	Career path survey in the cybersecurity and privacy industry 2024
Survey respondents	• Cybersecurity and privacy-related workers • Japanese and US residents • Organisation: Number of employees: 300 or more • Departments: Board of Directors, Sales, Operations Department, General Affairs, Administration, Human Resources, Public Relations, Procurement, Internal Audit, Corporate Planning, Labor Management, Legal Affairs, Consultants, Analysts/Researchers, Pre-sales, System Development, Development of Packaged Software and Middleware, Network Design and Construction, Operation/Monitoring/Technical Support/Maintenance, Research/Patent/Technical Marketing/Quality Control, Database System Network, Application Development, Information Security, Help Desk, Sales Engineers, etc. • Cybersecurity or privacy-related work experience: 1 year or more
Survey period	• Questionnaire survey: (Tuesday) 9 January 2024 to (Thursday) 18 January 2024 • Interview survey: (Wednesday) 17 April 2024 to (Friday) 10 May 2024
Survey method	• Questionnaire survey on the Internet • Interview survey
Number of questionnaire respondents	600 (US: 150 male, 150 female; Japan: 150 male, 150 female)

Appendix:
Respondent attributes and miscellaneous data

a. Respondent attributes

In conducting the survey, we received questionnaire responses from a total of 600 respondents comprised of 300 Japanese professionals and 300 US professionals working in the cybersecurity industry. A look at the respondents' attribute data (Figure 30) reveals that, among the industries in which the respondents' organisations belonged, the most common was the information and communications industry (including cybersecurity), followed by manufacturing, finance/insurance and wholesale/retail. Sixty-five percent of those organisations have more than 1,000 employees. In addition, roughly 80% of the survey's respondents earned their last degree by graduating from a university or graduate school (Figure 31). As for the locations of the respondents, it is apparent that the majority of Japanese respondents were located in Tokyo, while US respondents were distributed across various states (Figure 32). Percentages showing the attributes of organisations of affiliation (Figure 33), departments of affiliation (Figure 34) and employment status (Figure 35) are as indicated.

Figure 30: Respondents' attributes: (1) Country and gender, industry of organisation and number of employees of organisation

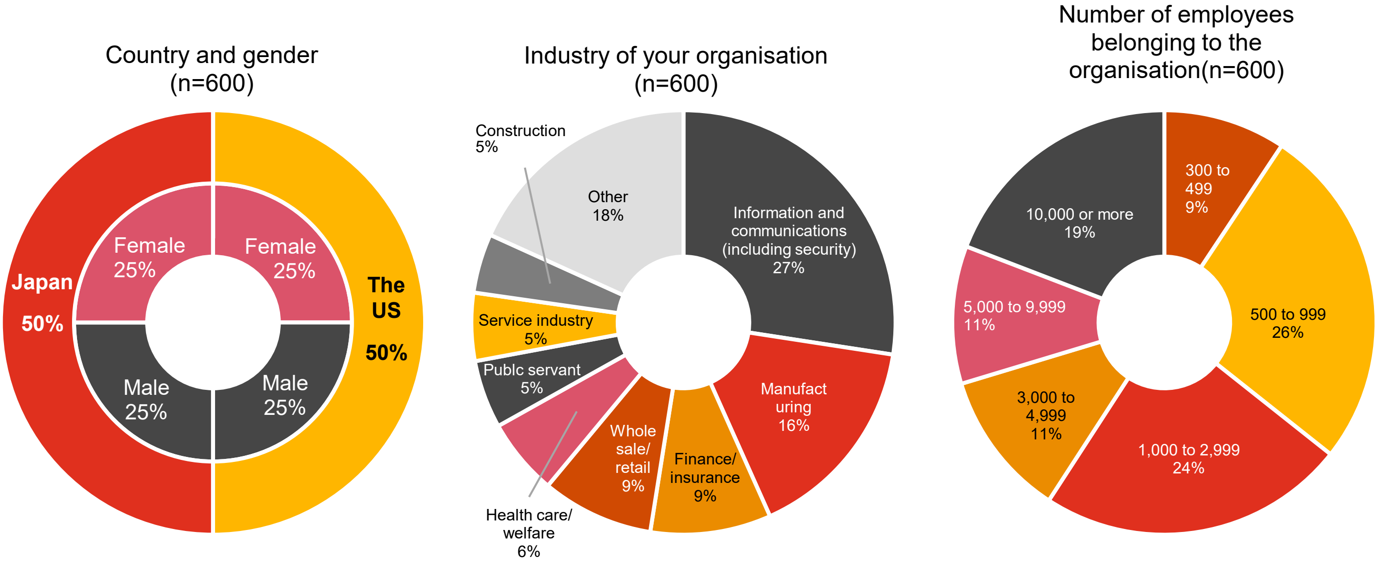


Figure 31: Respondents' attributes: (2) Academic background, years of work experience and focus of work

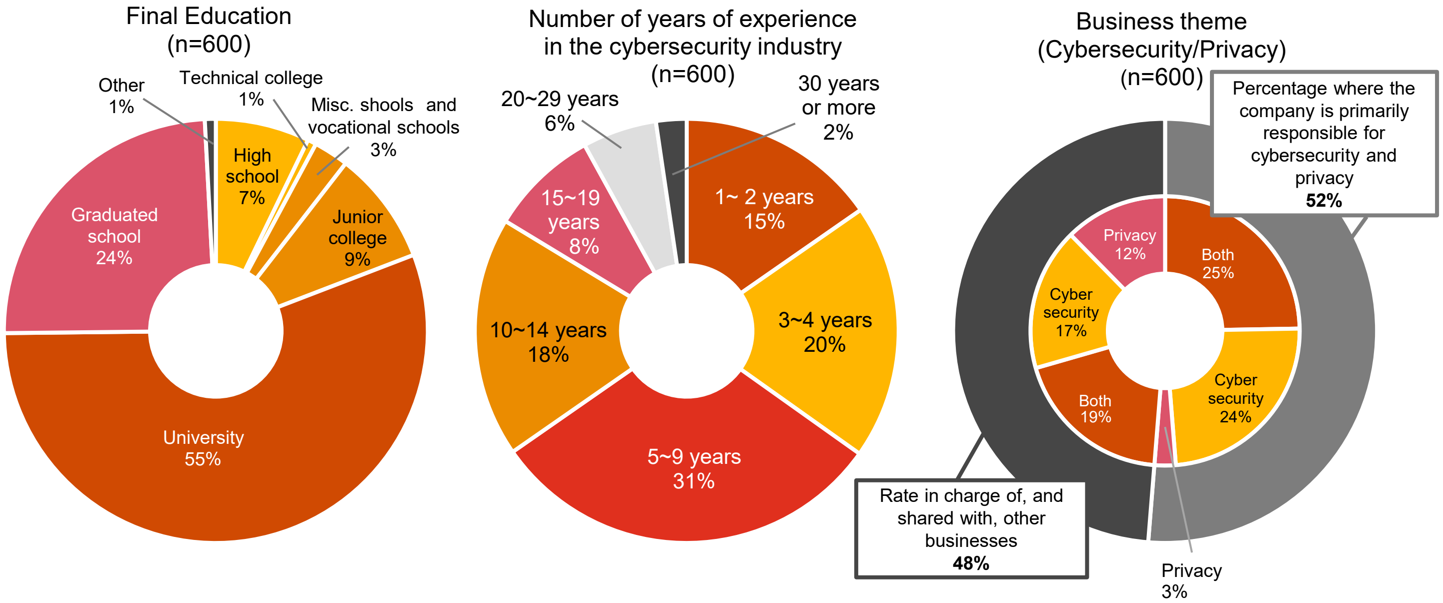
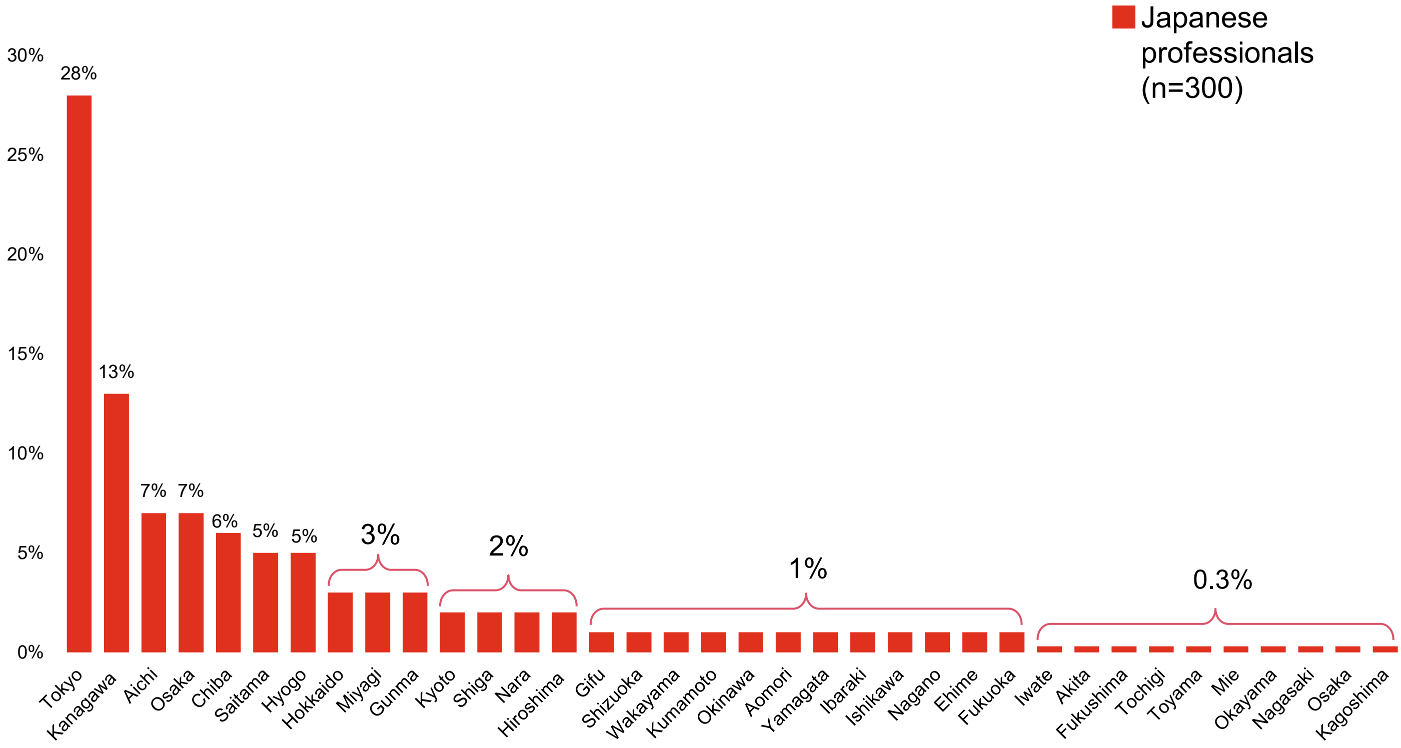


Figure 32: Respondents' attributes: (3) Location (Japan, US)



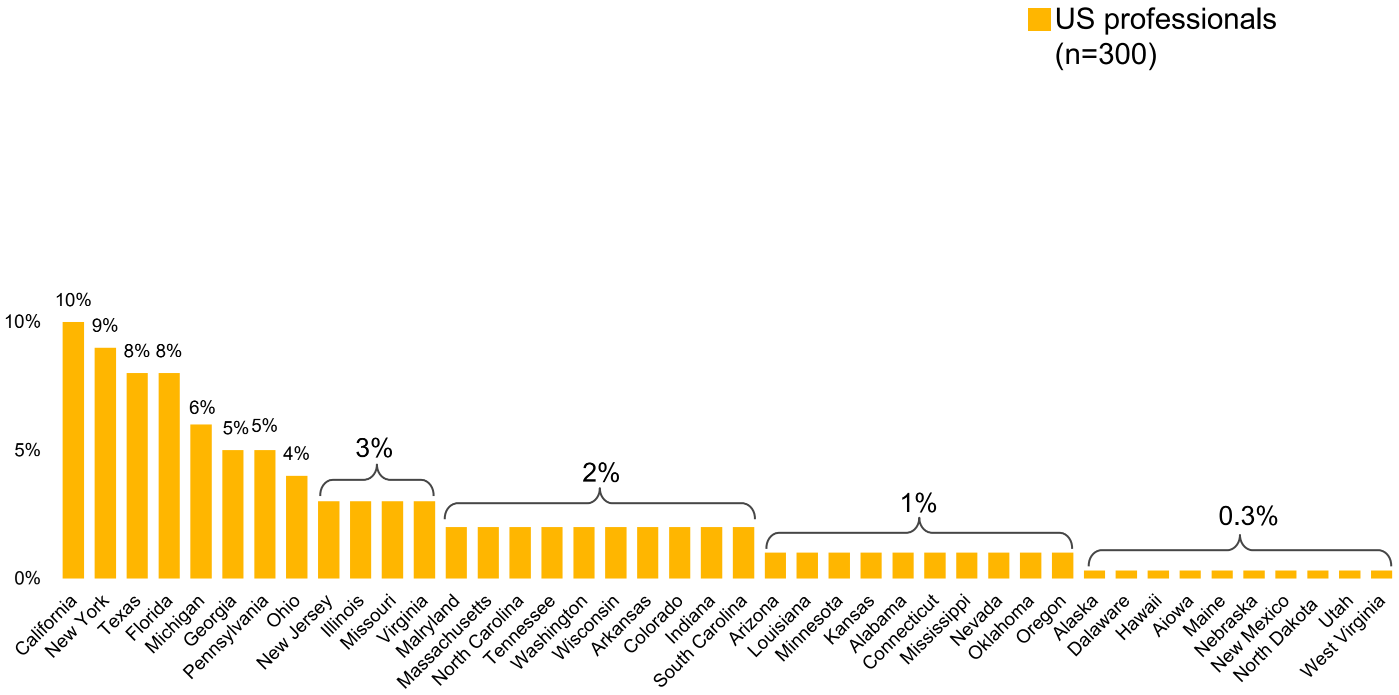


Figure 33: Respondents' attributes: (4) Attributes of company of affiliation (Japan, US: past, present)

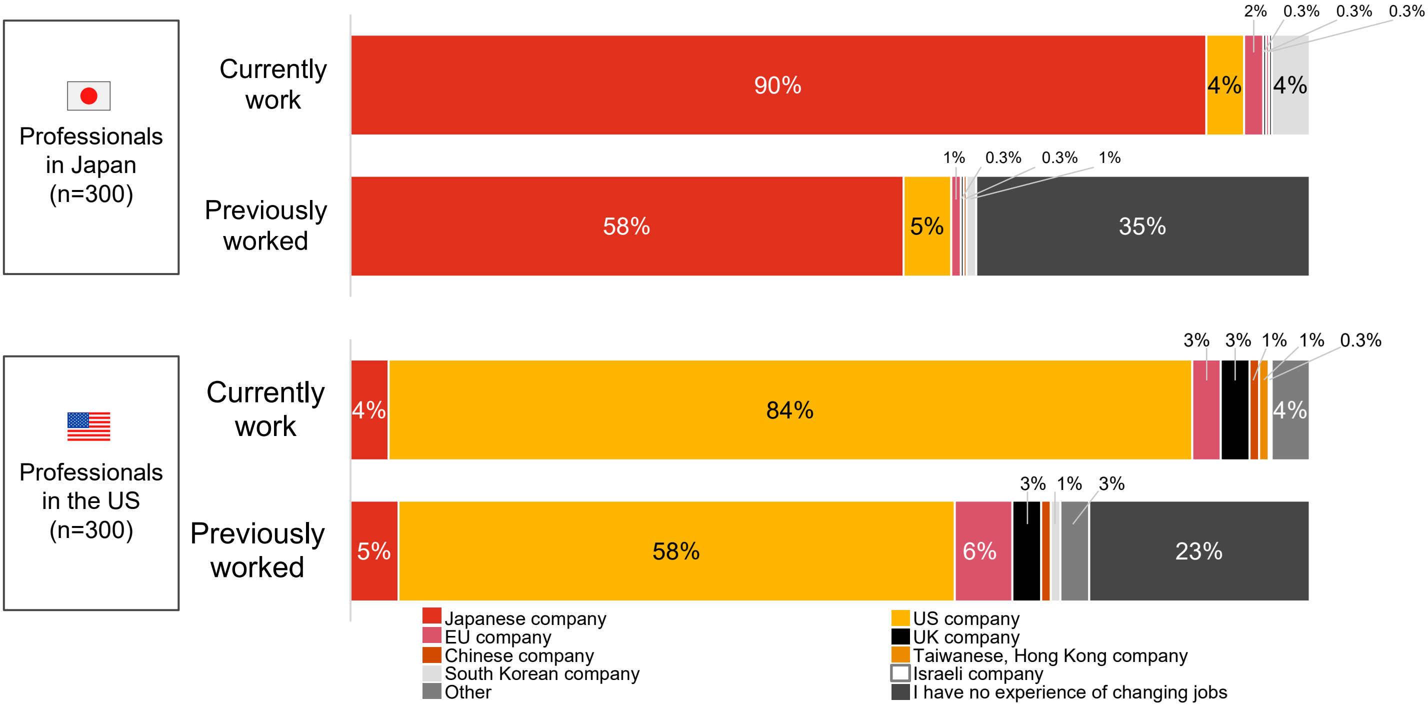


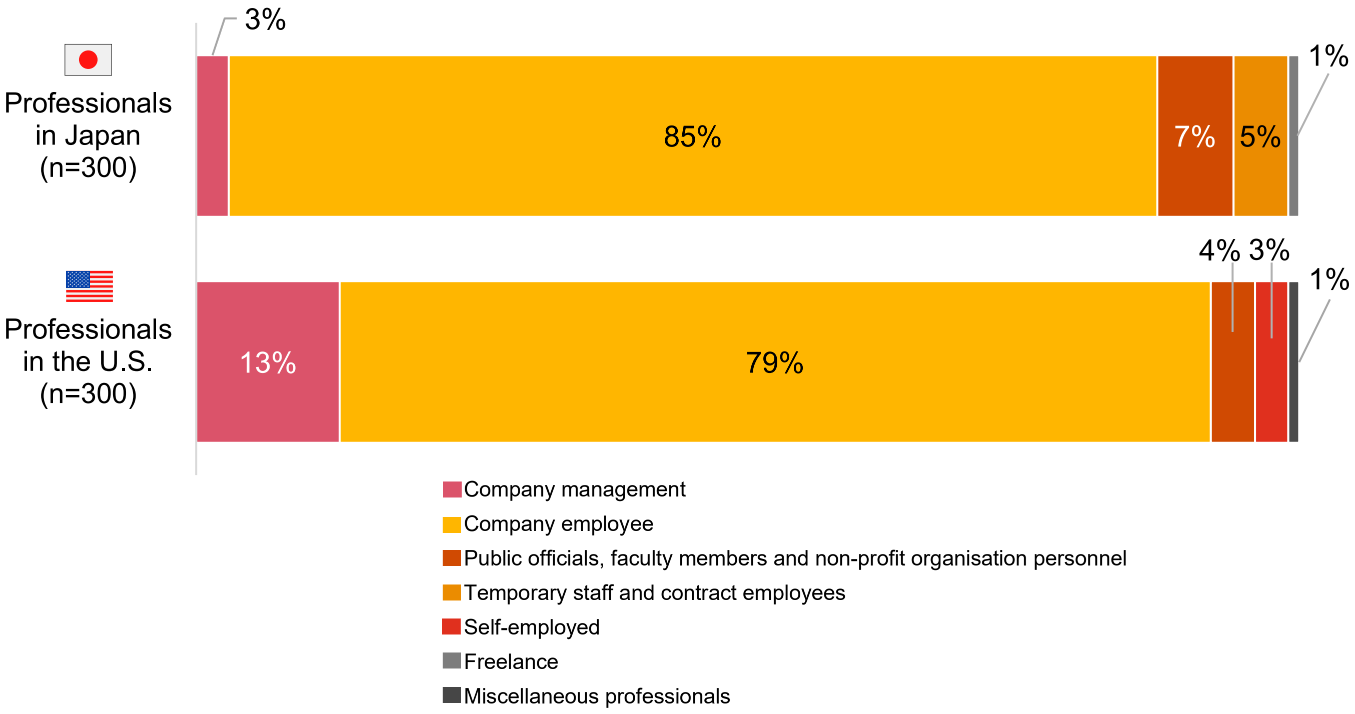
Figure 34: Respondents' attributes: (5) Department of affiliation

		Sales	General Affairs	Administration	Information Security	Human Resources	Operations Department	Board of Directors (Executive Level)	Operation, Monitoring, Technical Support, and Maintenance	System Development	Sales Engineer	Corporate Planning	Design and Construction of Telecommunication infrastructure	Legal Affairs	Development of Packaged Software and Middleware
Japan	Non-STEM	21%	15%	8%	7%	7%	5%	5%	5%	4%	3%	3%	2%	2%	2%
	STEM	7%	4%	9%	20%	1%	5%	4%	4%	14%	2%	0%	3%	0%	4%
The US	Non-STEM	8%	7%	11%	14%	8%	5%	8%	3%	2%	0%	2%	2%	4%	2%
	STEM	3%	2%	5%	34%	4%	5%	10%	3%	5%	0%	1%	3%	1%	2%

		Network Design, Construction	Databases, Systems and Networks	Application	Labour Management	Analysts/Researchers	Pre-sales	Internal Audit	Help Desk	Consultant	Procurement	Public Relations	Research, Patents, Technical Marketing, Quality Control, etc.	Other Occupations
Japan	Non-STEM	2%	1%	1%	1%	1%	1%	1%	1%	0%	0%	0%	0%	7%
	STEM	4%	3%	1%	1%	1%	1%	0%	0%	2%	2%	1%	1%	8%
The US	Non-STEM	2%	2%	2%	2%	2%	0%	2%	1%	2%	4%	1%	2%	7%
	STEM	1%	5%	2%	1%	1%	0%	1%	1%	5%	2%	2%	1%	2%

■ :30% or more ■ :20~29% ■ :10~19% ■ :5~9% □ :1~4% ■ :0%

Figure 35: Respondents' attributes: (6) Employment status



b. Other data

Other relevant data obtained from the survey is provided below. Please use the information as data points where necessary.

Figure 36: Percentage of females working in the cybersecurity industry (management, non-management): Japan

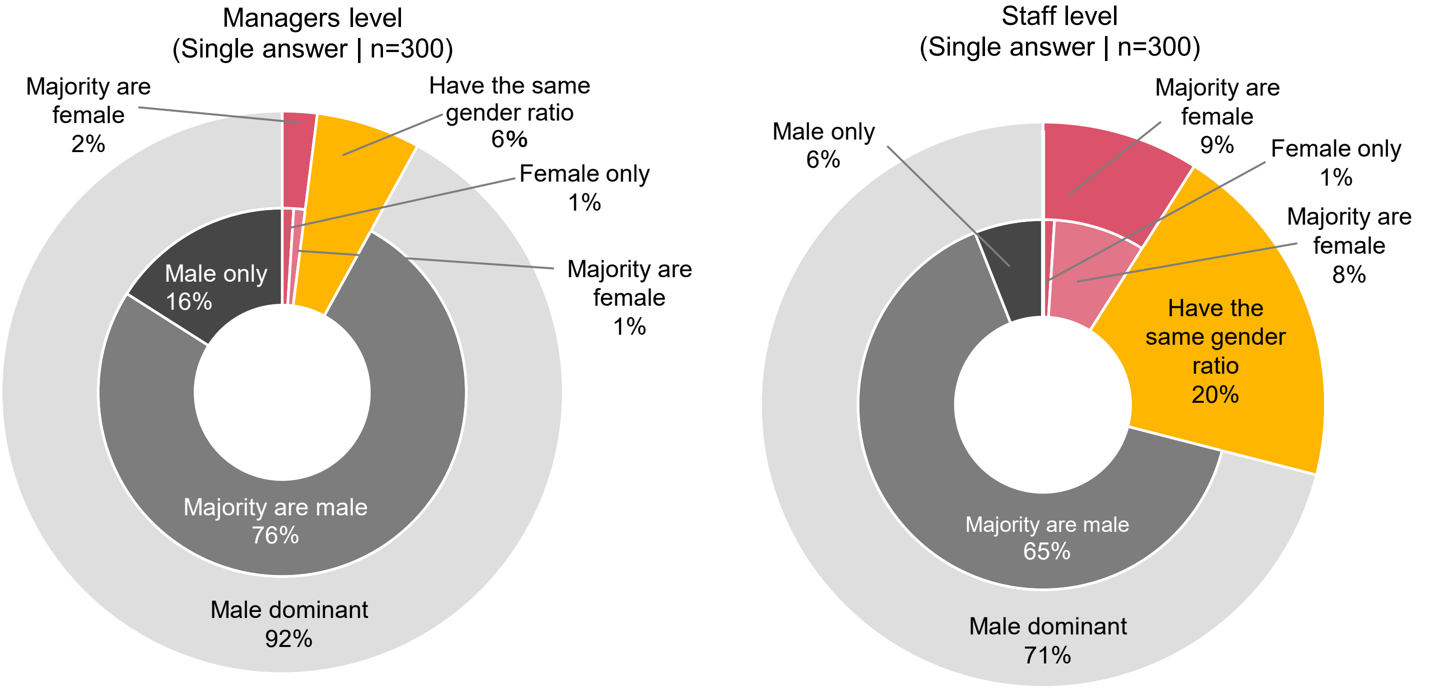


Figure 37: Percentage of females working in the cybersecurity industry (management, non-management): US

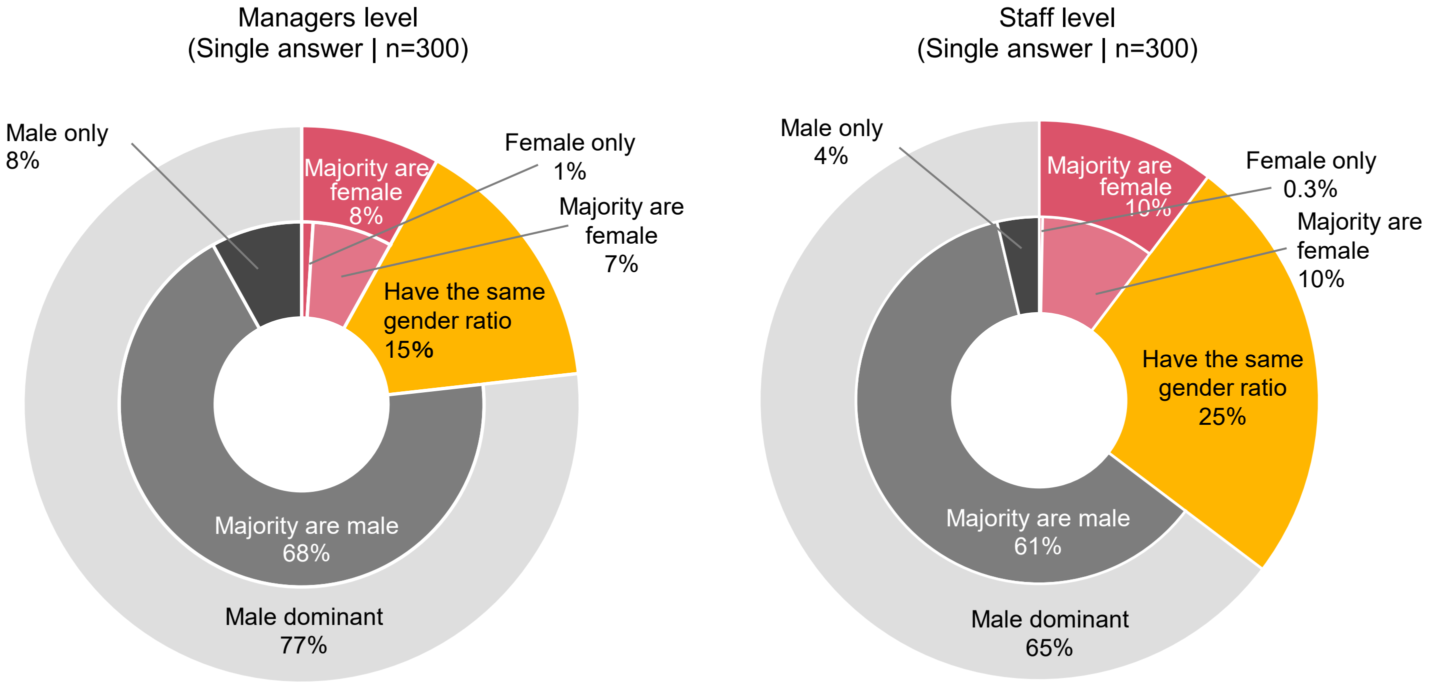


Figure 38: Initial reasons for involvement in cybersecurity and privacy work (Japan-US comparison)

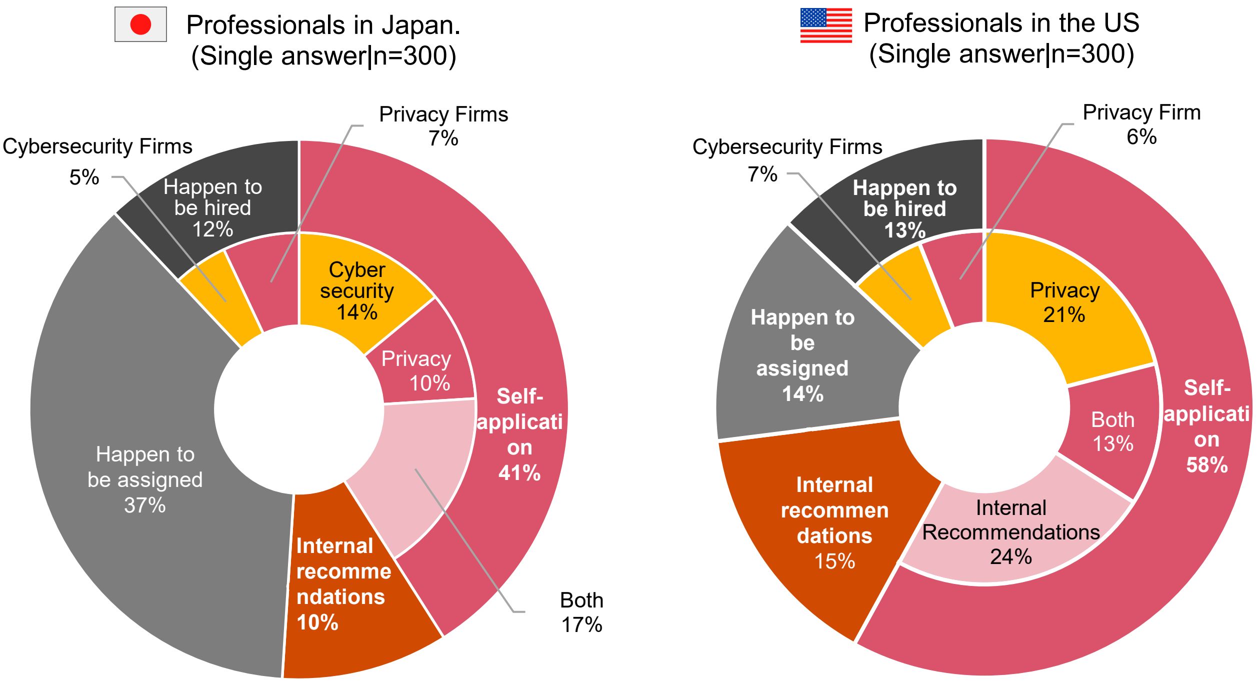
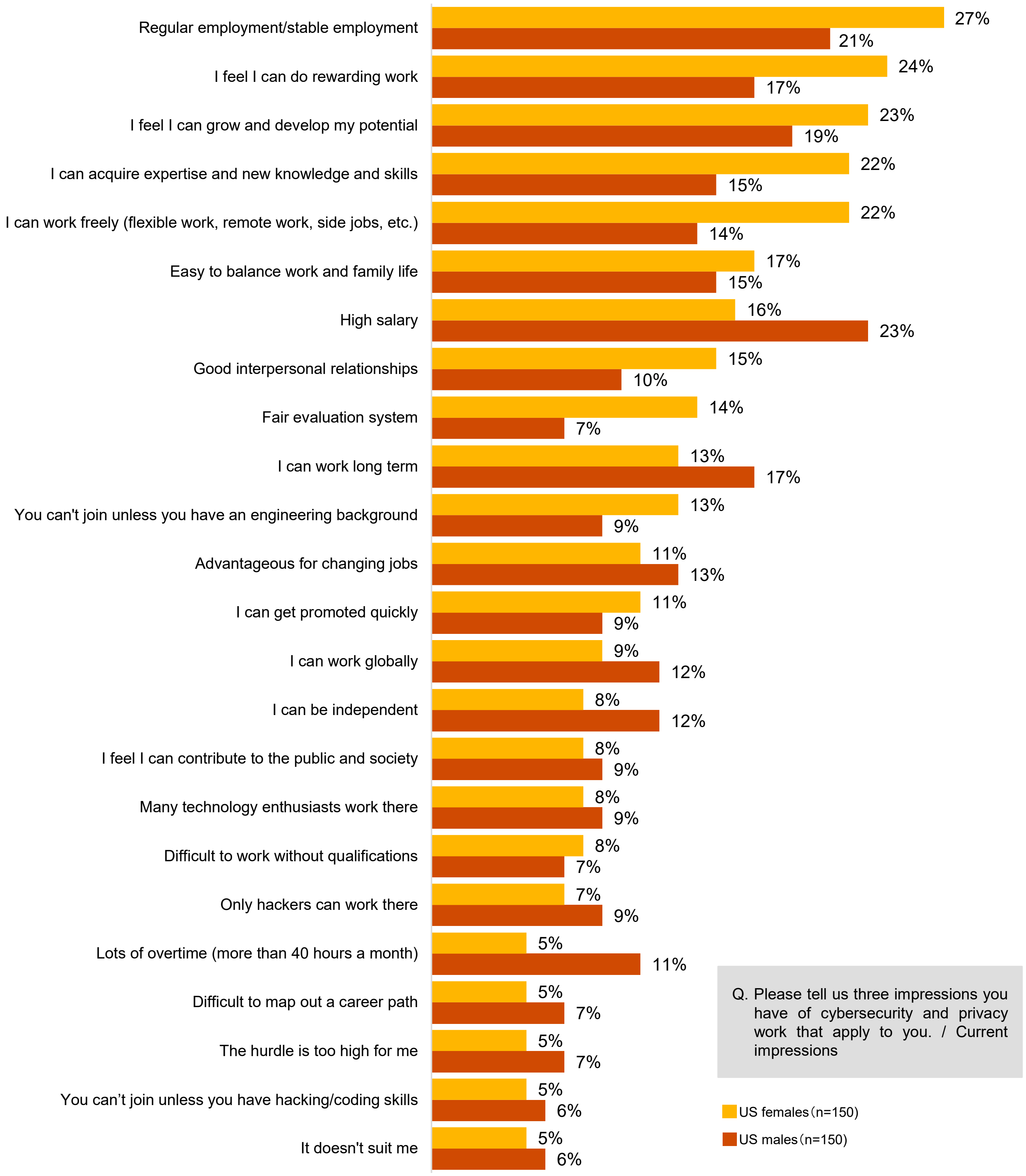
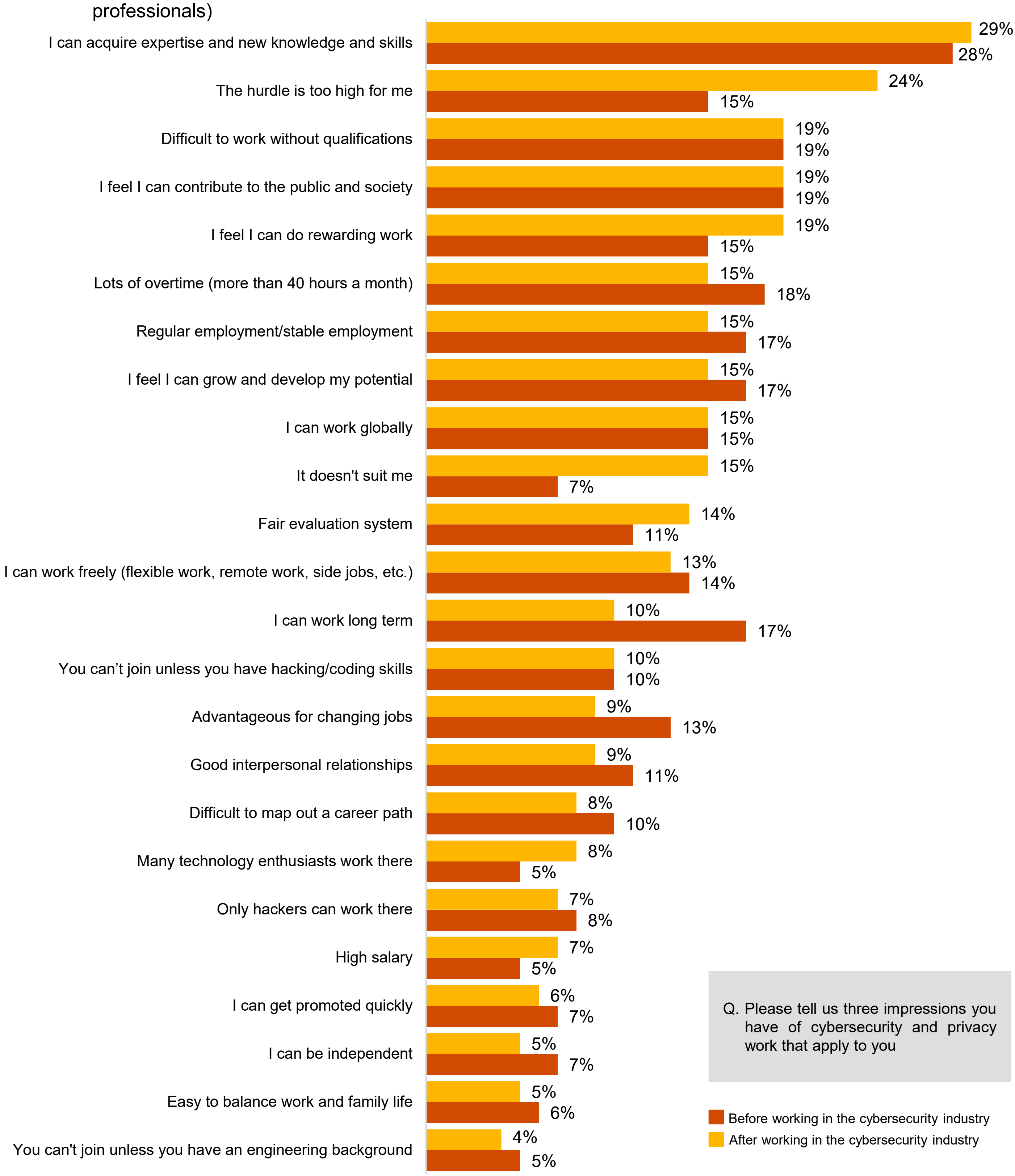


Figure 39: Comparison of impressions of the cybersecurity industry after ’ actually working in it (US professionals)



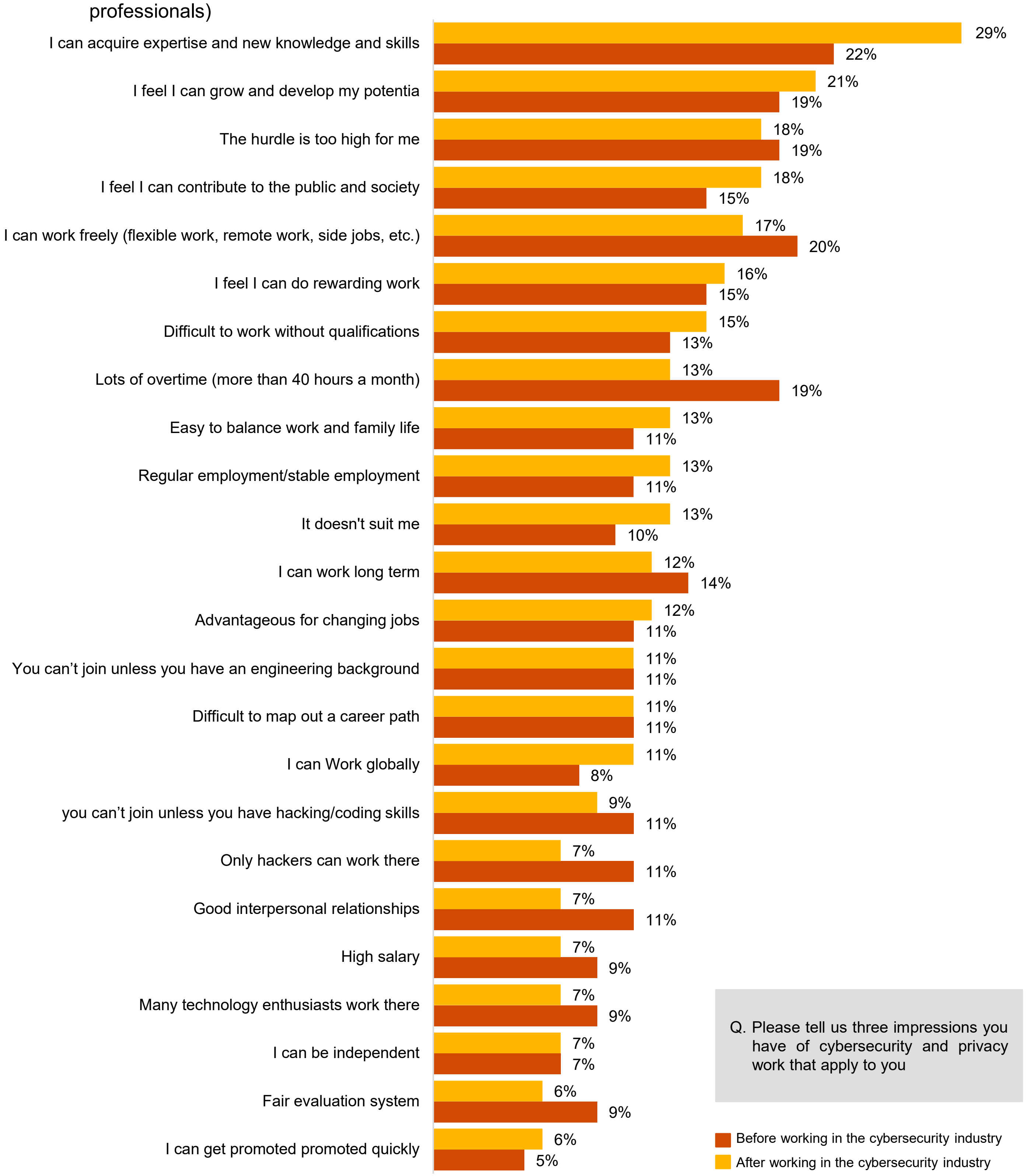
Q. Please tell us three impressions you have of cybersecurity and privacy work that apply to you. / Current impressions

Figure 40: Comparison of impressions of the cybersecurity industry before and after working in it (Japanese female professionals)



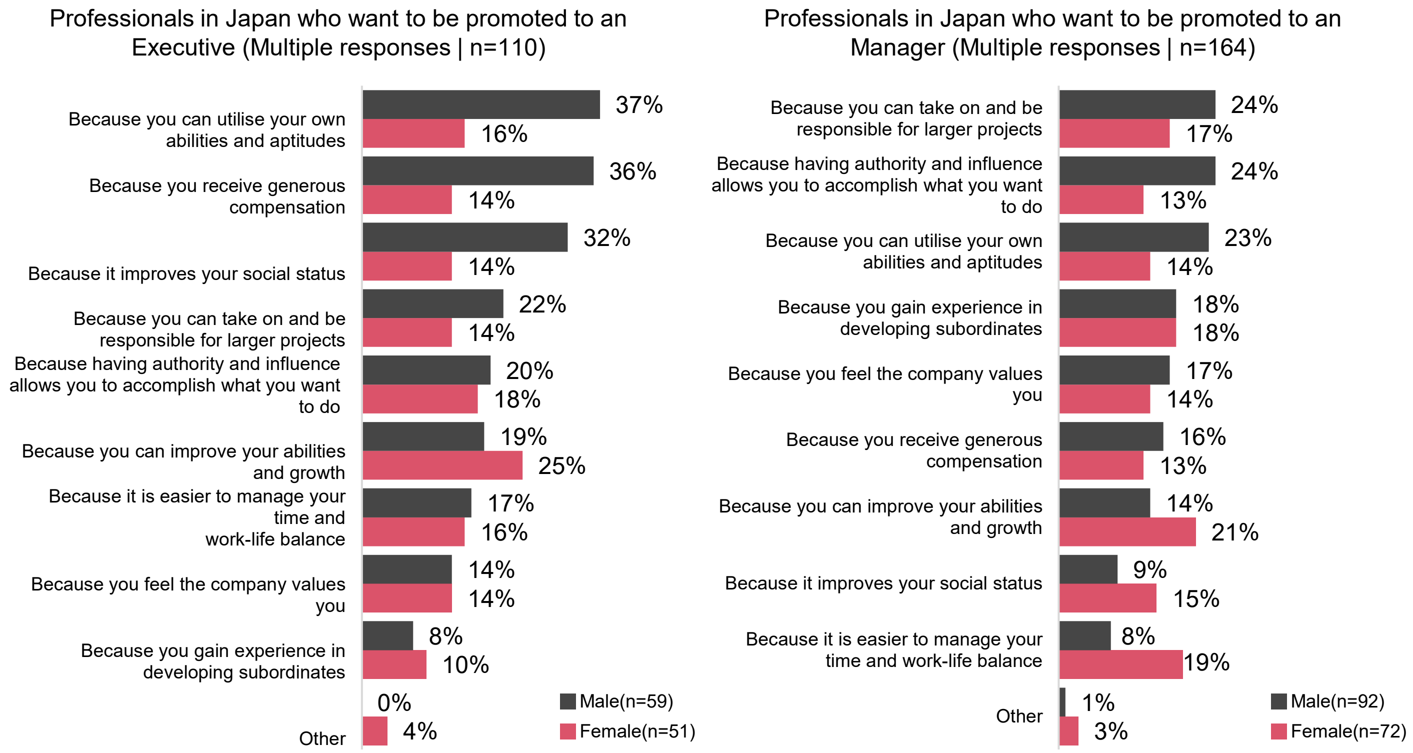
Q. Please tell us three impressions you have of cybersecurity and privacy work that apply to you

Figure 41: Comparison of impressions of the cybersecurity industry before and after working in it (Japanese male professionals)



Q. Please tell us three impressions you have of cybersecurity and privacy work that apply to you

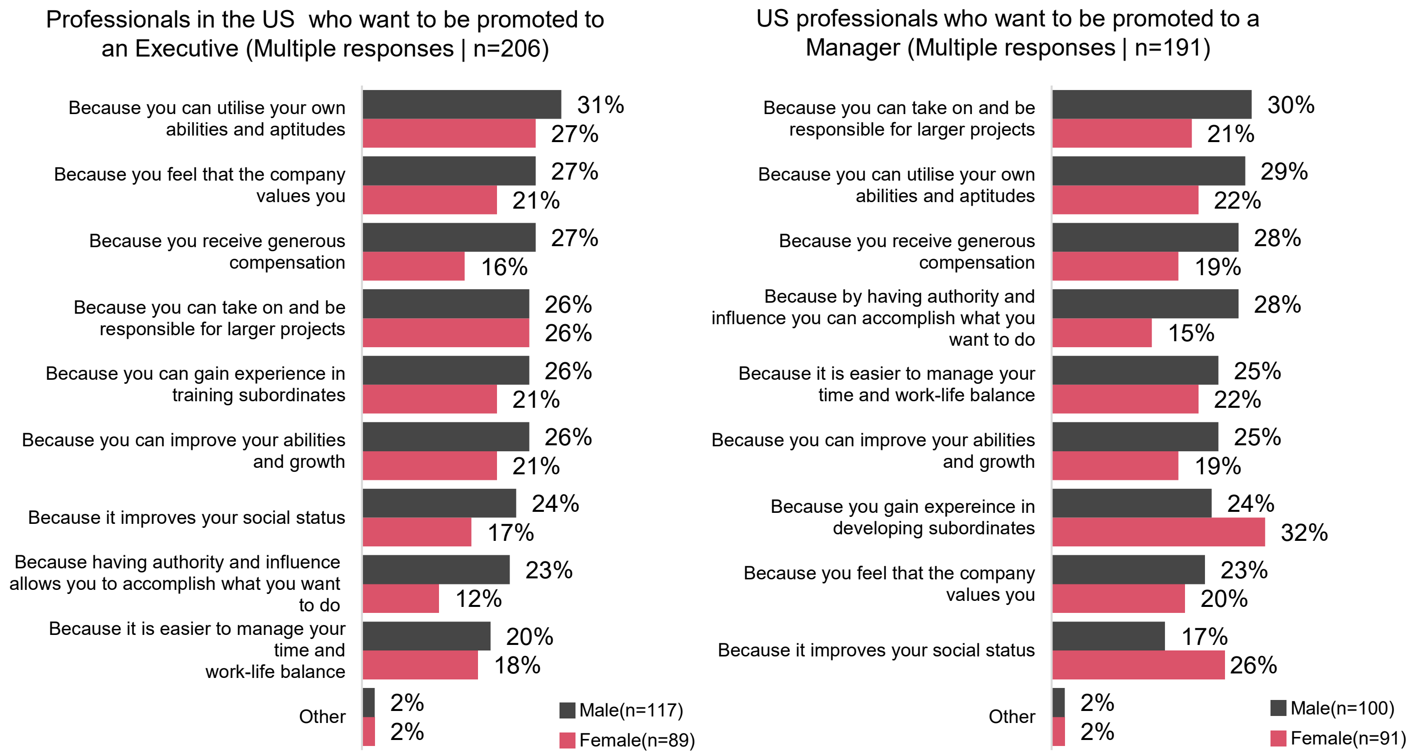
Figure 42: Reasons for desiring promotion (Japan)



Professionals in Japan who want to be promoted to an Executive (Multiple responses | n=110)

Professionals in Japan who want to be promoted to an Manager (Multiple responses | n=164)

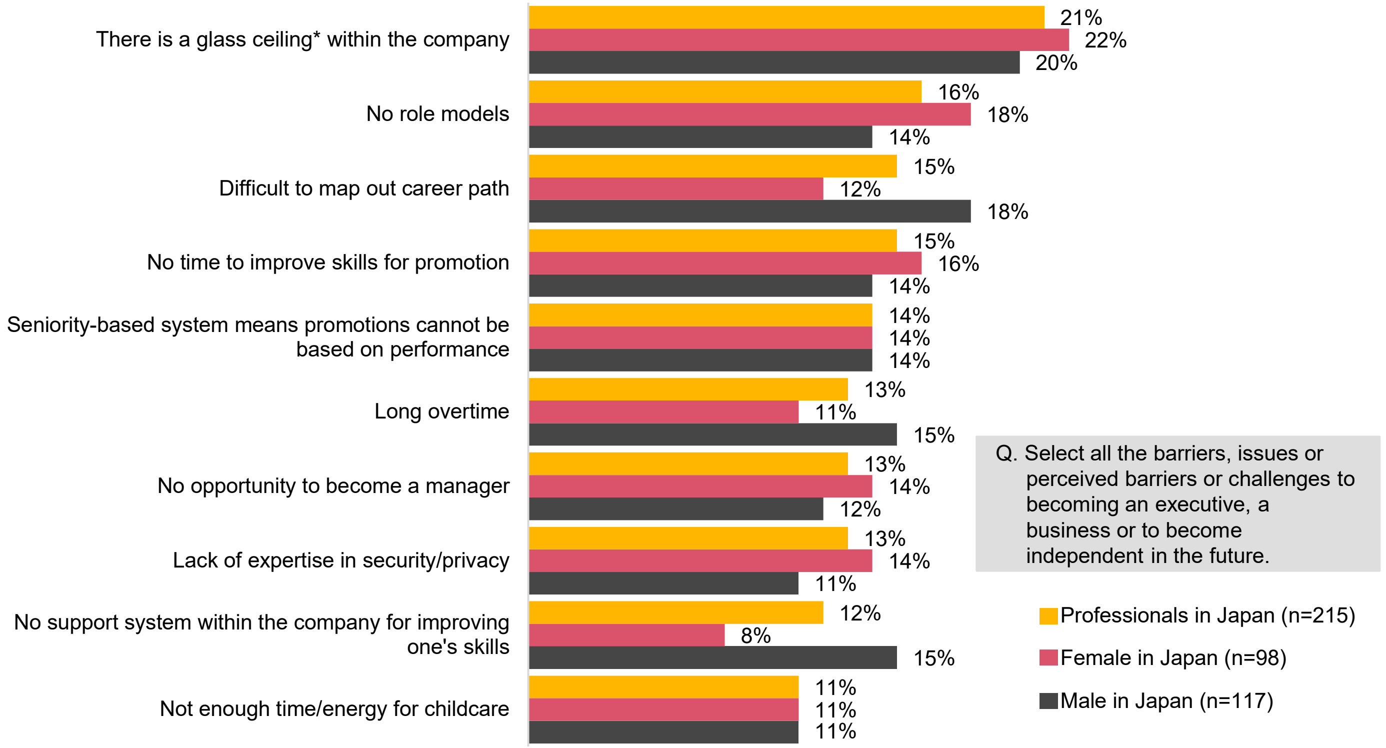
Figure 43: Reasons for desiring promotion (US)



Professionals in the US who want to be promoted to an Executive (Multiple responses | n=206)

US professionals who want to be promoted to a Manager (Multiple responses | n=191)

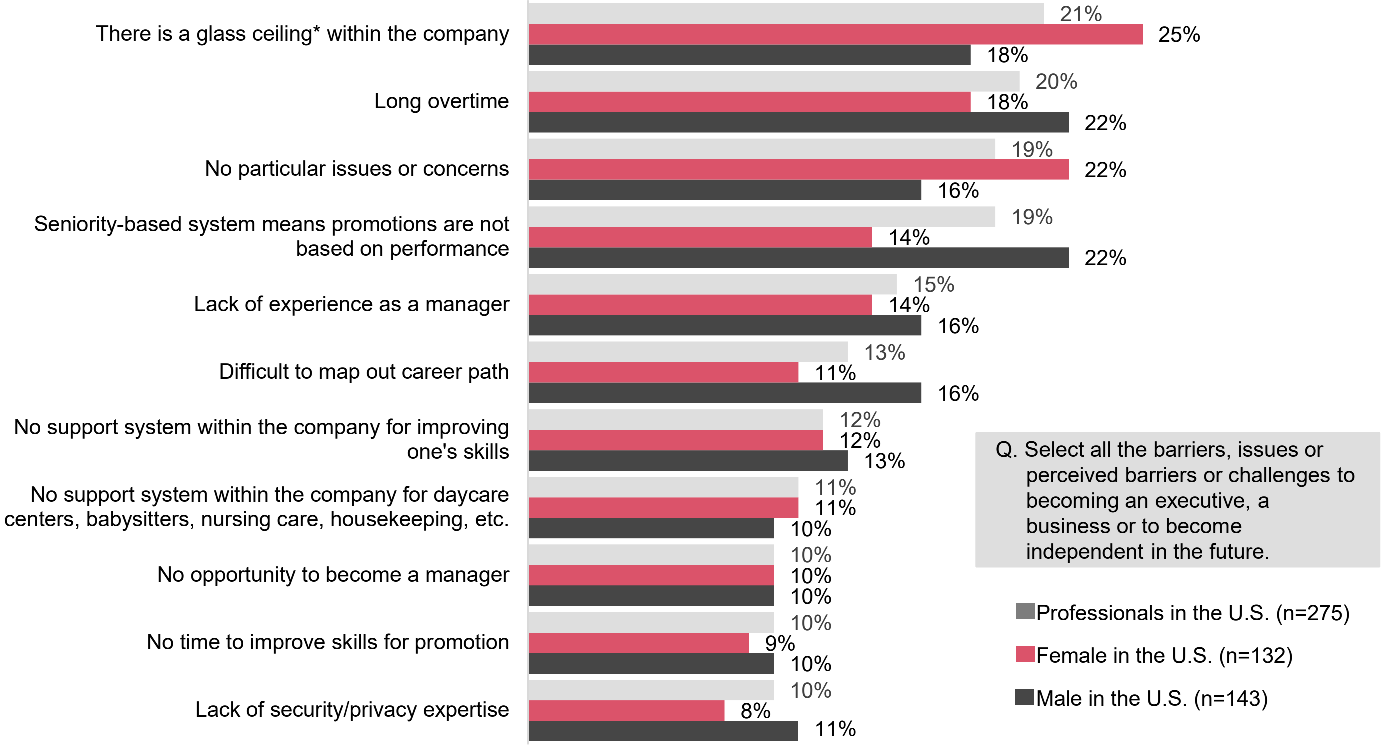
Figure 44: Concerns and challenges in getting promoted (Japan: top 10 responses)



Q. Select all the barriers, issues or perceived barriers or challenges to becoming an executive, a business or to become independent in the future.

* A situation in which a person is unable to advance to higher positions within an organisation despite having the ability and qualifications for promotion due to their gender or race. It is often used in situations where there are barriers preventing senior management roles from being accessible to certain groups.

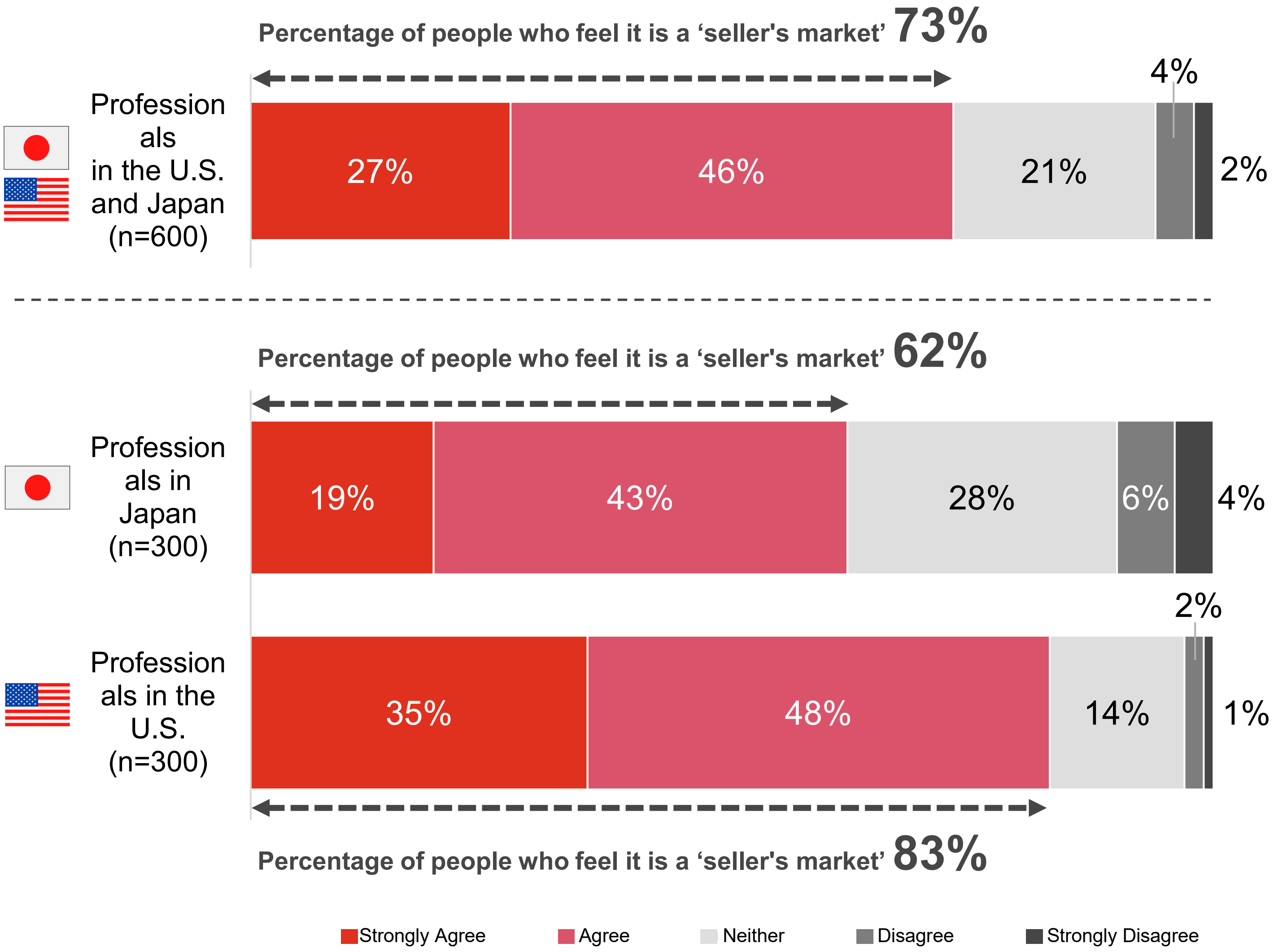
Figure 45: Concerns and challenges in getting promoted (US: top 10 responses)



Q. Select all the barriers, issues or perceived barriers or challenges to becoming an executive, a business or to become independent in the future.

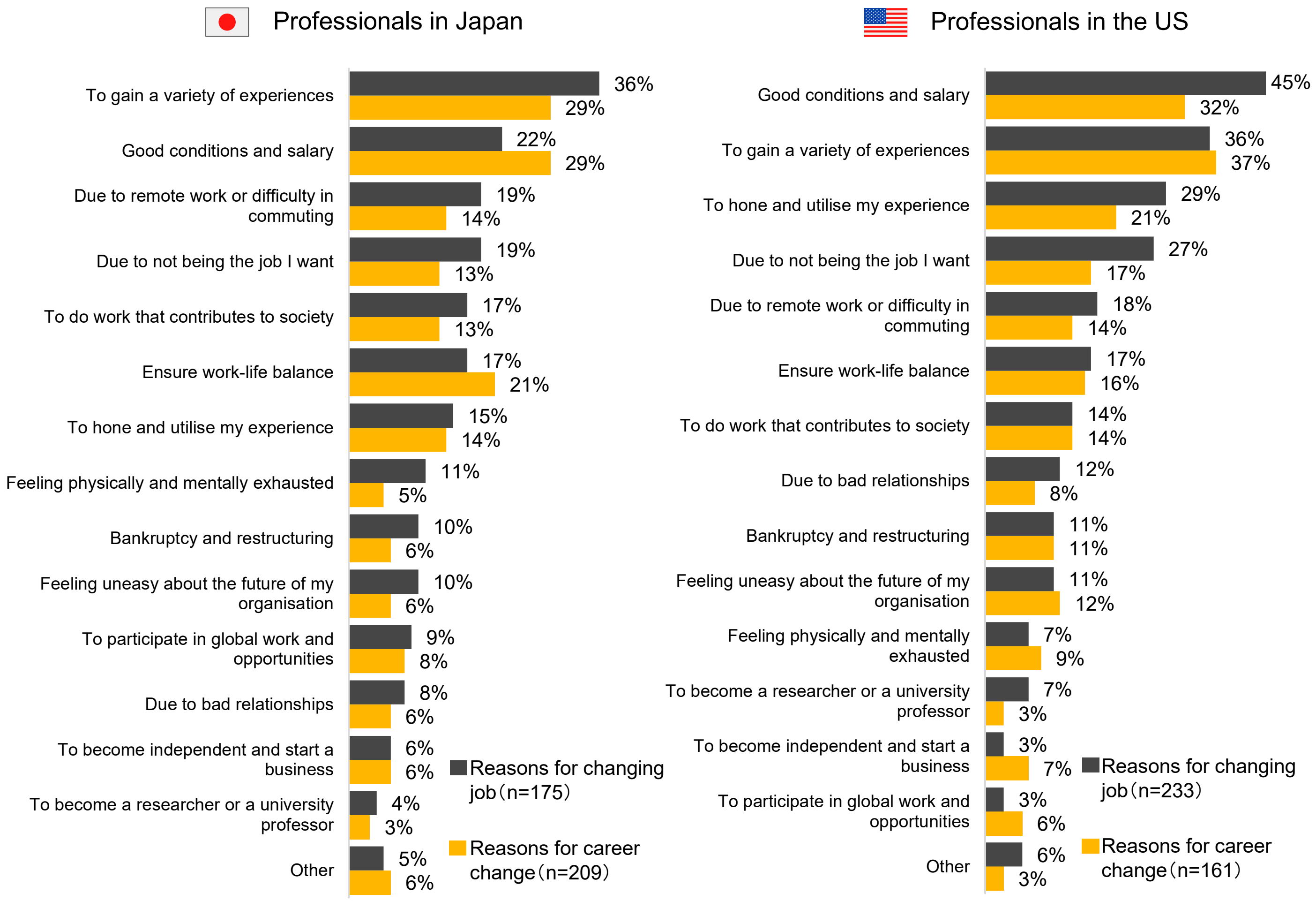
* A situation in which a person is unable to advance to higher positions within an organisation despite having the ability and qualifications for promotion due to their gender or race. It is often used in situations where there are barriers preventing senior management roles from being accessible to certain groups.

Figure 46: Percentage of respondents who feel that cybersecurity personnel are in a ‘seller’s market’ (Japan-US comparison)



Q. Do you think that people in the cybersecurity and privacy industry are in a ’seller’s market’ (in favour of finding and changing jobs)? What is most applicable?

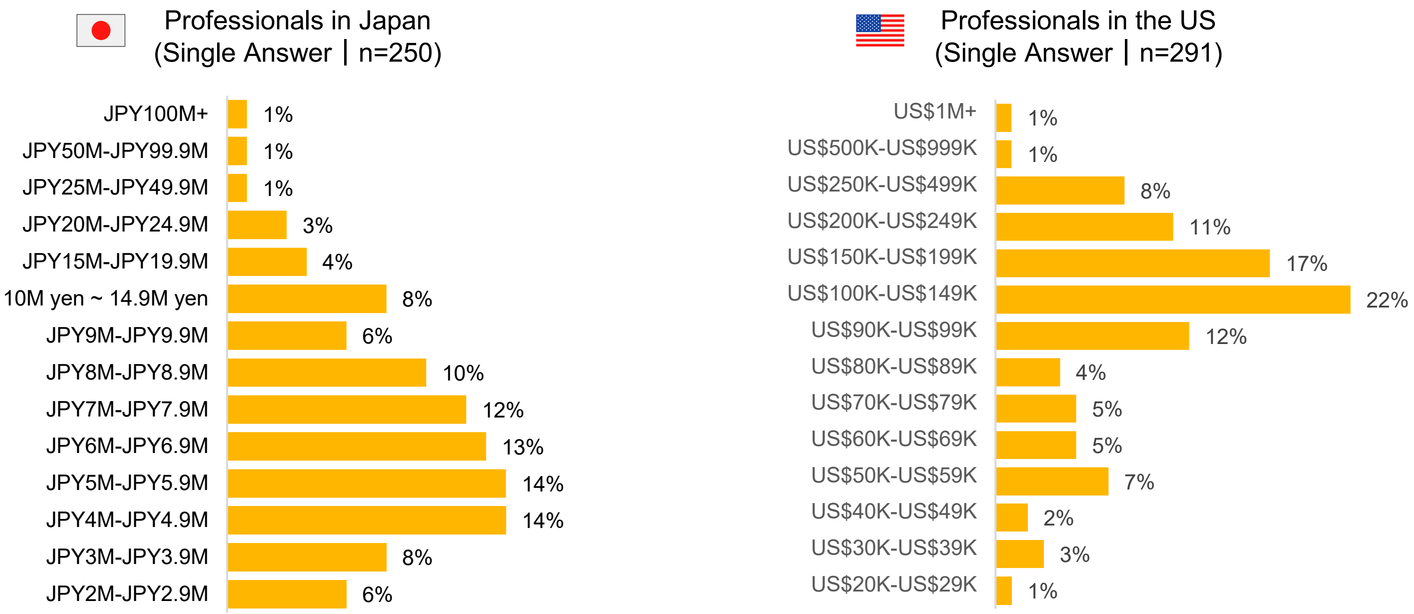
Figure 47: Percentages of past ‘reasons for career change’ and future ‘reasons for wanting a career change’ (Japan, US)



Professionals in Japan

Professionals in the US

Figure 48: Currently desired annual income (Japan-US comparison)



Professionals in Japan (Single Answer | n=250)

Professionals in the US (Single Answer | n=291)

Editor

Sean King

Partner, PwC Consulting LLC

Taiji Ayabe

Partner, Senior Executive Officer,
PricewaterhouseCoopers Japan LLC

Writers

Keiko Hayashi

Senior Manager, PwC Consulting LLC

Hiromi Aiko

Manager, PwC Consulting LLC

Kotomi Maki

Associate, PwC Consulting LLC

Contact us

PwC Japan Group
https://www.pwc.com/jp/en/contact.html

www.pwc.com/jp

The PwC Japan Group is a collective name for the member firms of the PwC global network in Japan and their affiliates. Each firm within the PwC Japan Group conducts its business as a separate, independent business entity. In response to our clients' increasingly complex and diverse corporate management issues, the PwC Japan Group has put in place a system that consolidates our knowledge in the fields of auditing and broader assurance services, consulting, deal advisory, tax and legal services, and encourages organic collaboration among our professionals in each field. As a professional services network with approximately 12,700 certified public accountants, tax accountants, lawyers and other professional staff, we strive to provide services that more accurately address our clients' needs.
At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with nearly 364,000 people who are committed to delivering quality in assurance, advisory and tax services.

The electronic version can be downloaded here. www.pwc.com/jp/ja/knowledge/thoughtleadership.html
Publication date : September 2024 (English Translation) Control No: I202407-03

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.