SIA

中國香港網絡安全協會
HONG KONG CHINA NETWORK SECURITY ASSOCIATION

The cybersecurity talent landscape in Hong Kong – a first study

A survey of cybersecurity professionals in Hong Kong to understand the current challenges in the cybersecurity workforce landscape and how they can be addressed in the future.

sia-partners.com

June 2025

Forewords of the HKCNSA Chairman

/ ADDRESSING HONG KONG'S CYBERSECURITY TALENT OUTFLOW: CHALLENGES AND LONG-TERM OPPORTUNITIES

As Chairman of the Hong Kong China Network Security Association (HKCNSA), I recognize the severe talent outflow in Hong Kong's cybersecurity sector, exacerbated by the COVID-19 pandemic. The city has faced a shrinking talent pool due to emigration, reduced foreign specialist inflows, and heightened demand for tech skills globally. This crisis threatens Hong Kong's position as a financial and tech hub, particularly as cyber threats grow in sophistication.

However, this challenge also presents opportunities to rebuild sustainably. First, deeper collaboration with universities is critical. While initiatives like HKUST's MoU with the HKMA on cybersecurity research are promising, academia-industry partnerships remain underdeveloped. Universities must expand applied programs, internships, and certifications to align curricula with industry needs.

Second, cross-industry collaboration — a core mission of HKCNSA — can pool resources and standardize training. The financial sector's partnership with academia on suptech and regtech innovations is a model for other industries.

Regaining competitiveness will take time, but Hong Kong has the infrastructure, regulatory frameworks, and global connectivity to succeed. By investing in homegrown talent and fostering ecosystem-wide collaboration, we can turn today's gap into tomorrow's strength.

Warm Regards,
David Ip
Founding Chairman
HKCNSA.

David Ip, Founding Chairman, Hong Kong China Network Security Association

Mr. David Ip is the Founding Chairman of the Hong Kong China Network Security Association. He is devoted to promoting the formulation and implementation of regulations and industry standards for cybersecurity and creating a favorable environment for the development of the industry.

David held senior positions in a number of leading global cyber security companies where he was responsible for strategic planning and market growth for the global market.

David holds a degree in Computer Science from University College London, UK. He is a frequent public speaker at global conferences, sharing his knowledge and experience in cybersecurity and China digital marketing.

/ Table of contents

02 Forewords of the HKCNSA Chairman

04 Introduction

05 The Methodology of this Study

06 The Structure of the Study

07 Acknowledgements

08 1. Context: An Overview of the Current Cybersecurity Workforce Market

11 2. Survey Findings: Insights from Cybersecurity Professionals, Recruiters and Universities

11 What is the situation in Hong Kong?

12 What is the impact of the talent shortage?

16 How effective is talent acquisition in Hong Kong?

18 What are universities doing to support the future cybersecurity talents?

20 What are organizations doing to face the current challenges?

23 What are the salary expectations?

24 What motivates candidates to have a cybersecurity career?

26 How much companies are investing in cybersecurity?

27 Are there unique challenges for cybersecurity talent in Hong Kong?

29 3. Looking at other countries in Asia: The case of Singapore

31 4. What's next: Conclusions and Future Outlook

31 Key considerations

33 Recommendations for the Future

35 Appendix

35 Survey Participants by Industry

35 Survey Participants by Organization Size in Hong Kong

The cybersecurity talent and workforce situation has been the subject of much discussion and research, especially following the Covid-19 pandemic.

There is a general consensus, supported by solid research and facts, that the workforce market is facing several challenges, notably a **significant imbalance between demand and supply**.

Hong Kong is not immune to this situation, and there is a widespread struggle to find the right resources, particularly when they are most needed. **Cybersecurity incidents and attacks are on the rise**, driven by increasingly sophisticated cybercriminals, with advancements in Artificial Intelligence enhancing both the speed and complexity of these attacks.

In recognition of this significant challenge, the HKCNSA aims to **deepen the understanding** of the current cybersecurity workforce in Hong Kong. The goal is to identify key root causes and trends, leading to **recommendations and actionable ideas** for stakeholders, including cybersecurity professionals, universities, government bodies, and others.

While many reports and studies on this topic exist globally, this is the **first attempt** to provide clarity on such a complex issue within the Hong Kong community. The local context presents similarities with other markets but also has its unique characteristics.

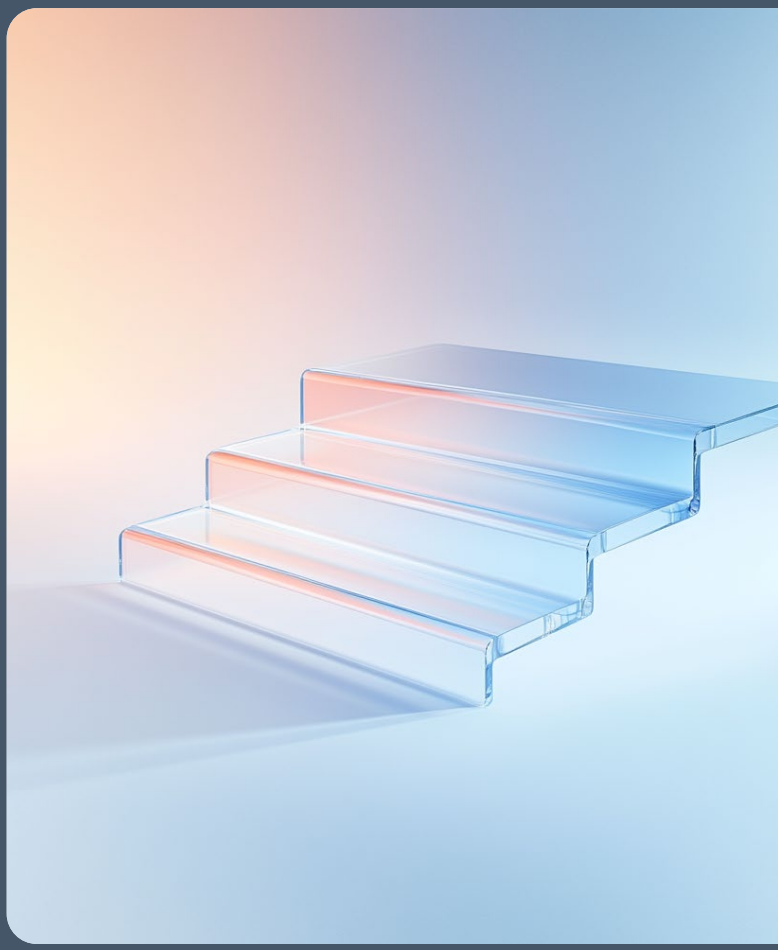
Understanding these trends and phenomena is essential for the cybersecurity community in Hong Kong, which aims to **ensure a secure and stable digital landscape** across all applications and domains. The HKCNSA is actively involved in the community, not only to connect various professionals but also to educate and raise awareness about key industry challenges. The Association promotes continuous improvement and practices that enhance the security of digital services.

We aim to continue this research in the coming years and closely monitor the cybersecurity talent landscape in Hong Kong on a regular basis. This will allow us to observe how the situation evolves and assess the effectiveness of various initiatives and recommen-dations.

The Methodology of this Study

The HKCNSA has collaborated with **Sia**, on the preparation and publication of this study, which aims to explore the current cybersecurity talent landscape in Hong Kong.

The research has been conducted through a **dedicated survey by contacting around a hundred of cybersecurity professionals in Hong Kong**, asking direct questions about their perspectives on hiring and retaining cybersecurity talent within their organizations. The survey has explored the impacts of the current workforce shortage, how organizations are coping with it, and their expectations for the future. Additionally, complementary inquiries were made with a handful of **professional recruiters** who possess a broad understanding of the talent market and can provide valuable insights.



During the study, the **current academic landscape** was also examined, exploring what universities in Hong Kong are doing to educate and prepare the next generation on cybersecurity matters.

A short study was also conducted on **current initiatives by the Hong Kong government**, particularly the **Hong Kong Talent Engage** program, to understand the activities being undertaken related to cybersecurity and the outlook for the future.

Furthermore, a brief comparison with the context in **Singapore** has been included in this research to highlight similarities and differences, as well as to identify potential best practices to consider.

The Structure of the Study

The study is composed of four main parts:

Part 1. Context: An Overview of the Current Cybersecurity Workforce Market

This section gives a short description of what is going on in the cybersecurity workforce market today, sharing some figures at global and regional level, identifying the key macro trends in the cybersecurity domain, as well as the specificities of Hong Kong in this context.

Part 2. Survey Findings: Insights from Cybersecurity Professionals, Recruiters and Universities

This section details the results of the survey conducted among cybersecurity professionals in Hong Kong. It includes quantitative data on hiring practices, skills shortages, and retention challenges. Additionally, complementary comments and insights from top cybersecurity professionals and recruiters offer a qualitative perspective, highlighting key trends and obstacles faced in the local market. Furthermore, this section provides insight into what universities in Hong Kong are doing regarding cybersecurity courses and programs for graduate and postgraduate students.

Part 3. Looking at other countries in Asia: the case of Singapore

This section provides a brief picture of the cybersecurity landscape in Singapore. Key highlights include Singapore's successful initiatives in talent development and retention, which may serve as potential models for Hong Kong to consider.

Part 4. What's next: Conclusions and Future Outlook

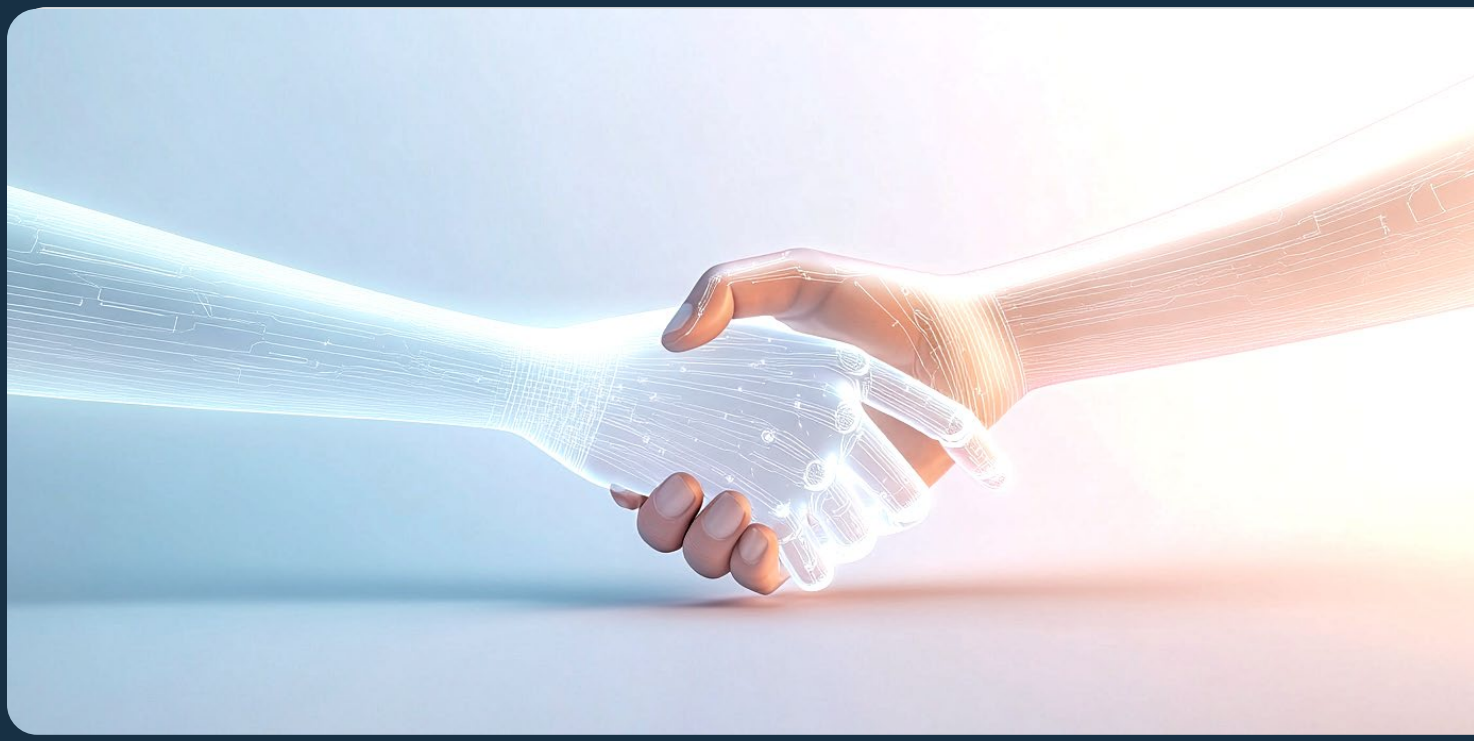
This section summarizes the key findings and provides strategic recommendations for stakeholders in Hong Kong's cybersecurity sector. It outlines the anticipated outlook for the talent landscape, emphasizing the need for collaborative efforts between industry and academia. High-level suggestions include enhancing training programs, fostering partnerships with educational institutions, and implementing policies to attract and retain skilled professionals.

Acknowledgements

We would like to express our gratitude to everyone who contributed to this study, especially the professionals in the cybersecurity industry who took the time to complete the surveys, answer our questions, and share their insights. Without their participation, this study would not have been possible.

First of all, we would like to thank **Prof. Philip Lee** (Assistant Professor at Hong Kong Shue Yan University) for his collaboration in designing and delivering the survey. In addition, we would like to thank the professio-nal recruiters, in particular **Fiona Fung** and **Isha Hussain** (Robert Walters), **Kelvin Chu** (Rands-tad), **Jackie Chow** (Hays) and **Elmer Tan** (Eames Consulting) to have shared their insights and knowledge about the Hong Kong and Singapore workforce market.

Furthermore, we would like to thank **Silvia Ihensekhien** (Group CISO & DPO at Swire Coca Cola), **Frankie Tam** (Partner at Eversheds Sutherland), **Bosco Tsin** (Lecturer at Hong Kong Shue Yan University), **Prof. Weiyin Hong** (Associate Professor at Hong Kong University of Science and Technology), **Chris Tse** (Instructional Designer at Hong Kong University of Science and Technology), **Prof. Yan Xu** (Professor at Hong Kong University of Science and Technology), **Anthony Lau** (Director of Hong Kong Talent Engage) and **Wilson Tang** (Vice Chairman of HKCNSA) for their time to add relevant feedback and insight to this study.



1. Context: An Overview of the Current Cybersecurity Workforce Market

The cybersecurity landscape in Hong Kong has reached a critical juncture, marked by a paradoxical surge in cyber threats alongside a widening talent gap.

In 2024, the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) handled 12,536 security incidents, with phishing cases doubling to 7,811 incidents — the **highest in five years**[1]. Concurrently, ransomware attacks targeting critical infrastructure, healthcare, and educational institutions have intensified[2]. These threats are exacerbated by the rapid **adoption of Artificial Intelligence** by attackers, enabling sophisticated phishing campaigns and deep-fake fraud.

The global cybersecurity sector faces a **deep talent crisis** with an estimated 4.8 million workforce gap despite 5.5 million active professionals worldwide[3]. This deficit leaves 47% of organizational cybersecurity needs unmet, exacerbating vulnerabilities in an era where cyberattacks cost the global economy $10.5 trillion annually[4]. While the Asia Pacific region hosts the largest share of cybersecurity professionals globally, **Hong Kong mirrors these challenges** with unique local complexities.

Official sources regarding the city's cybersecurity workforce indicate that there were 1,587 professionals in 2022, accounting for only 1.4% of the total IT

(1) HKCERT Unveils "Hong Kong Cyber Security Outlook 2025" Phishing Hits Five-year High Vulnerabilities in Supply Chain and AI Content Hijacking Emerge as Key Risks Over Half of Enterprises Fear Cyber Attacks on IoT Digital Signages, HKCERT, 20 January 2025
(2) Ransomware's New Front: Uncovering the Latest Threats Facing Hong Kong, HKCERT, 14 August 2024
(3) 2024 Cybersecurity Workforce Study, ISC2
(4) 2021 Report: Cyberwarfare In The C-Suite, Cybercrime Magazine

workforce[5]. While this figure may underestimate the current cybersecurity workforce in Hong Kong, there is a general consensus and concern about the lack of cybersecurity resources. The **gap appears to be widening** due to the increasing number of attacks and the introduction of new, more stringent regulations and compliance requirements, such as the recently released Critical Infrastructure Ordinance.

The shortage of cybersecurity talent may be a contributing factor to the deterioration of the cybersecurity posture in Hong Kong. In late 2023, the "Hong Kong Enterprise Cyber Security Readiness Index and Privacy Awareness" report was released, showing an alarming decline, with the **Cyber Security Readiness Index** dropping 6.3 points to 47/100 in 2023, making its largest decline since inception. The index gives an indication of the preparedness of enterprises to face cyber threats, and the worse indicators were identified for Small and Medium Enterprises, as well as for companies outside the Financial Services sector[6].

Based on expert opinions, the challenges facing the territory reflect global trends with distinct regional characteristics. Several key drivers have been identified that may influence the situation:

/ **Talent Exodus:** During and after the COVID-19 pandemic, many individuals, both expatriates and locals, have relocated to other countries, along with companies that have decided to close their Hong Kong offices.

/ **Regulatory Pressures:** New legislation, such as the Protection of Critical Infrastructures Ordinance, passed on March 2025, intensifies the demand for compliance expertise, which is lacking among a si-gnificant majority of local professionals.

/ **Educational Gaps:** While a few universities offer dedicated cybersecurity programs, partnerships with corporations appear to be underdeveloped.

This talent crisis persists despite the visible efforts and strategic initiatives pursued by the **Hong Kong Talent Engage** office (HKTE). HKTE aims to attract global talent, including those in cybersecurity and I&T, to develop their careers in Hong Kong, by identifying key overseas markets with concentrated talent pools and conducts targeted promotion campaigns. In addition, HKTE partners with top local universities and industry orga-nizations to host recruitment activities.

> "During its visit to Australia in March, HKTE promoted Hong Kong's advantages while accompanied by an Australian cybersecurity expert who has relocated to Hong Kong. The expert shared first-hand settlement experiences and career pathways with students and alumni of Australia's top universities."
>
> **Anthony Lau**
> Hong Kong Talent Engage

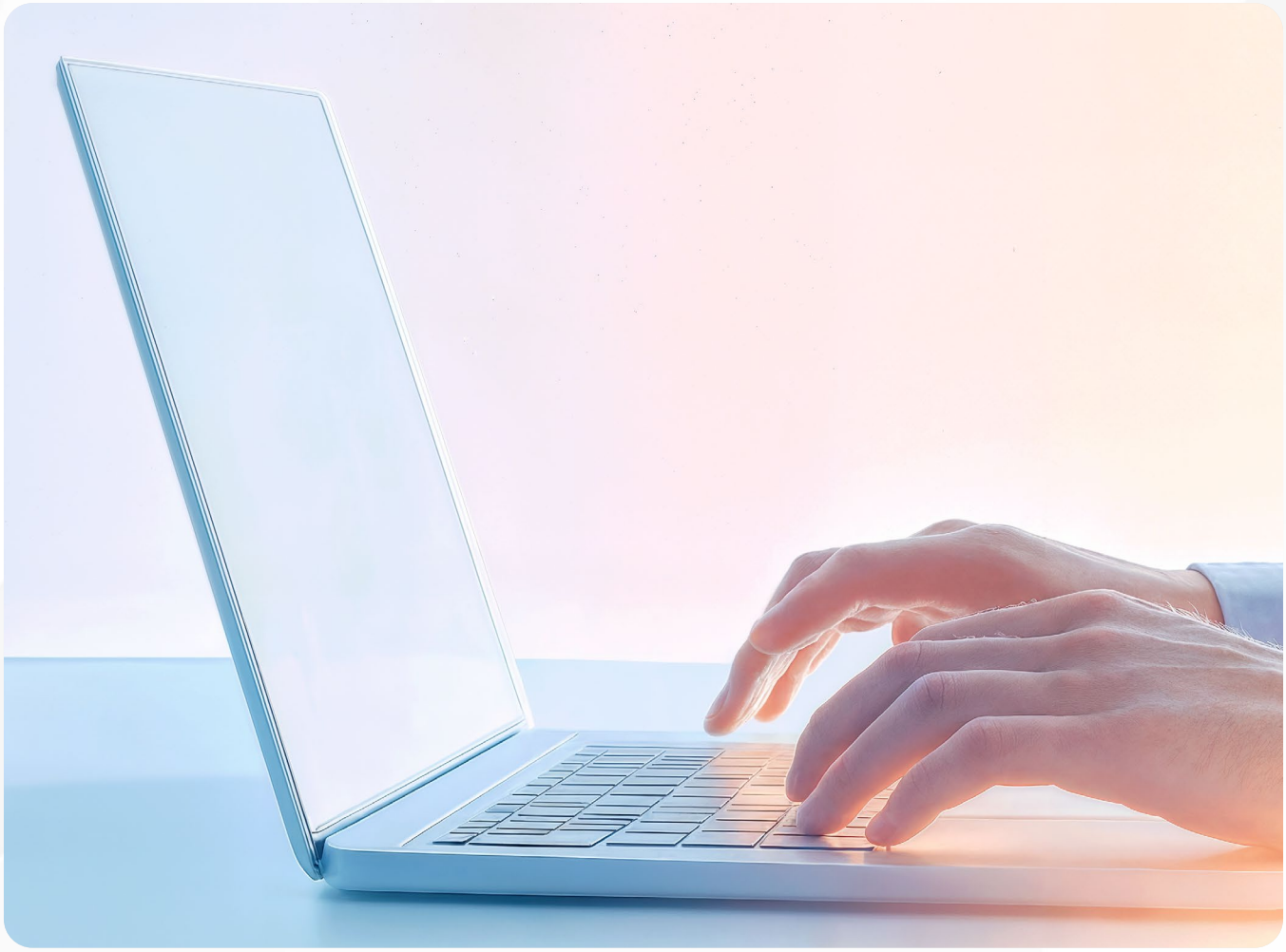
(5) 2022 Manpower Survey Report Innovation and Technology Sector, Innovation and Technology Training Board
(6) Hong Kong Enterprise Cyber Security Readiness Index and Privacy Awareness, Hong Kong Productivity Council Cyber Security, 2023

Recent research indicates that several areas need to be addressed to bridge this gap in the coming years, including improving academic programs, implementing gender diversity initiatives to enhance the participation of women in the cybersecurity workforce, and integrating AI skills[7].

As Hong Kong positions itself as Asia's digital finance hub, addressing these workforce challenges is imperative to safeguard its corporate community and maintain strong competitiveness in the region.

> "The gender gap in cybersecurity is an important issue. A balanced gender workforce can significantly enhance practices within the field. While many companies have made substantial strides in this area, it should not be viewed as a static target; rather, it is a long-term journey that requires ongoing effort and dedication. Initiatives should start in schools and universities, where women need encouragement and mentorship from an early stage."

Silvia Ihensekhien
Swire Coca Cola



(7) The BCG Global Cybersecurity Workforce Report

2. Survey Findings: Insights from Cybersecurity Professionals, Recruiters and Universities

What is the situation in Hong Kong?

In order to obtain a more accurate and direct understanding of the current context, a dedicated survey was sent to over a hundred top professionals in Hong Kong. **Most participants come from the financial services industry** (~40%), while other sectors such as manufacturing, technology, and transportation are also represented. For more details about the scope of the participants, please see the Appendix.

According to the responses, the majority of cybersecurity leaders believe their teams are **moderately to slightly understaffed, operating at about 75% of optimal capacity**.

A closer analysis reveals that **Incident Response Specialists** are the hardest roles to fill, followed by Governance, Risk and Compliance Specialists and Threat Intelligent Analysts as third most challenging role to fill.

CHARTE : HOW WOULD YOU RATE YOUR ORGANIZATION'S CURRENT CYBERSECURITY WORKFORCE NEEDS?

42% **Slightly understaffed** (<25% below optimal)

33% **Moderately understaffed** (25-50% below optimal)

17% **Adequately staffed**

8% **Severely understaffed** (>50% below optimal)

– **Overstaffed**

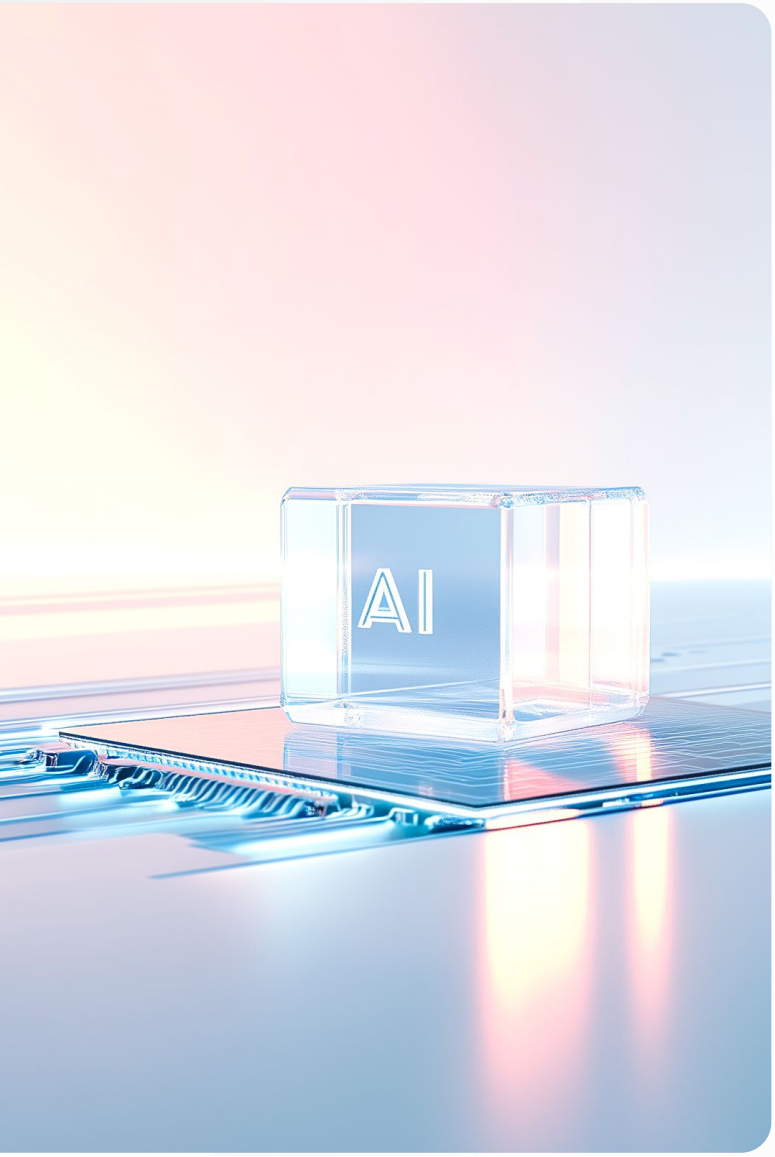


CHART 2: WHICH CYBERSECURITY ROLES ARE MOST CHALLENGING TO FILL IN YOUR ORGANIZATION?

If we look at the feedback of professional headhunters, they all agree that Hong Kong faces a significant shortage of cybersecurity professionals, with demand exceeding supply. Companies are responding by offering competitive packages and, on some occasions, trying to relocate talent from Southeast Asia, and investing in training junior candidates.

They all emphasize the need for specialized technical skills, including **cybersecurity engineering, cloud security, incident response**, and emerging areas like **AI security**.

Professional recruiters agree that the imbalance between demand and supply was also caused by the exodus of talent over the past five years. The Covid-19 crisis prompted both expatriates and Hong Kong locals to relocate to countries such as the UK and Singapore.

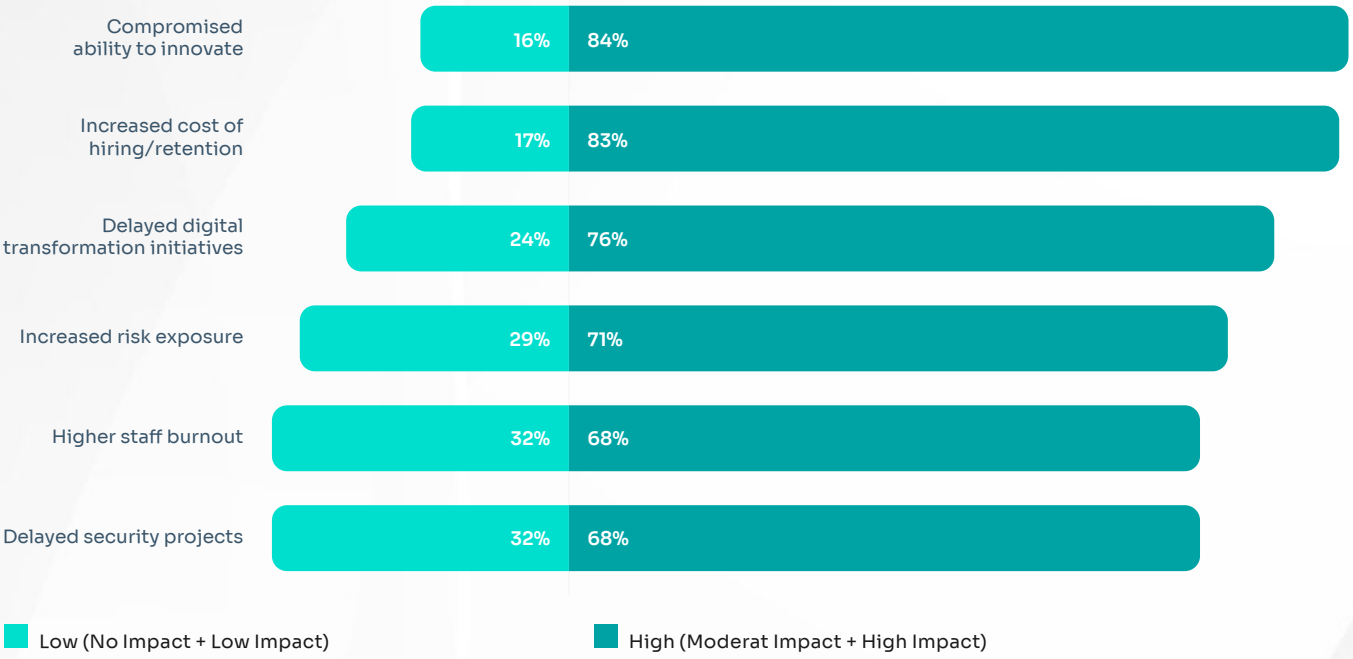
> “The shortage is particularly noticeable in areas like cloud security, AI security, and the red teaming, where hands-on experience is crucial.”
>
> **Jacky Chow**
> Hays

What is the impact of the talent shortage?

This staffing shortage and the challenges in finding qualified candidates have negatively impacted cybersecurity activities. Most participants agree that the greatest impact is the **ability to innovate**. Additionally, this situation has significantly **increased cost of hiring and retention** and the ability to **deliver key projects**, in particular in digital transformation.

Participants’ responses indicate that **security projects have been delayed** due to a lack of resources and the absence of qualified personnel. This context has also hindered the ability to anticipate and effectively address security incidents.

CHART 3: HOW HAS THE CYBERSECURITY TALENT SHORTAGE AFFECTED YOUR ORGANIZATION?



In light of the recent Protection of Critical Infrastructures Ordinance, concerns about the lack of qualified talent are evident. Most responses highlight that **Compliance Monitoring and Reporting, Supply Chain Security Management** and **Incident Reporting** present the highest challenges in terms of talent requirements.

CHART 4: IN YOUR OPINION, HOW LIKELY ARE:

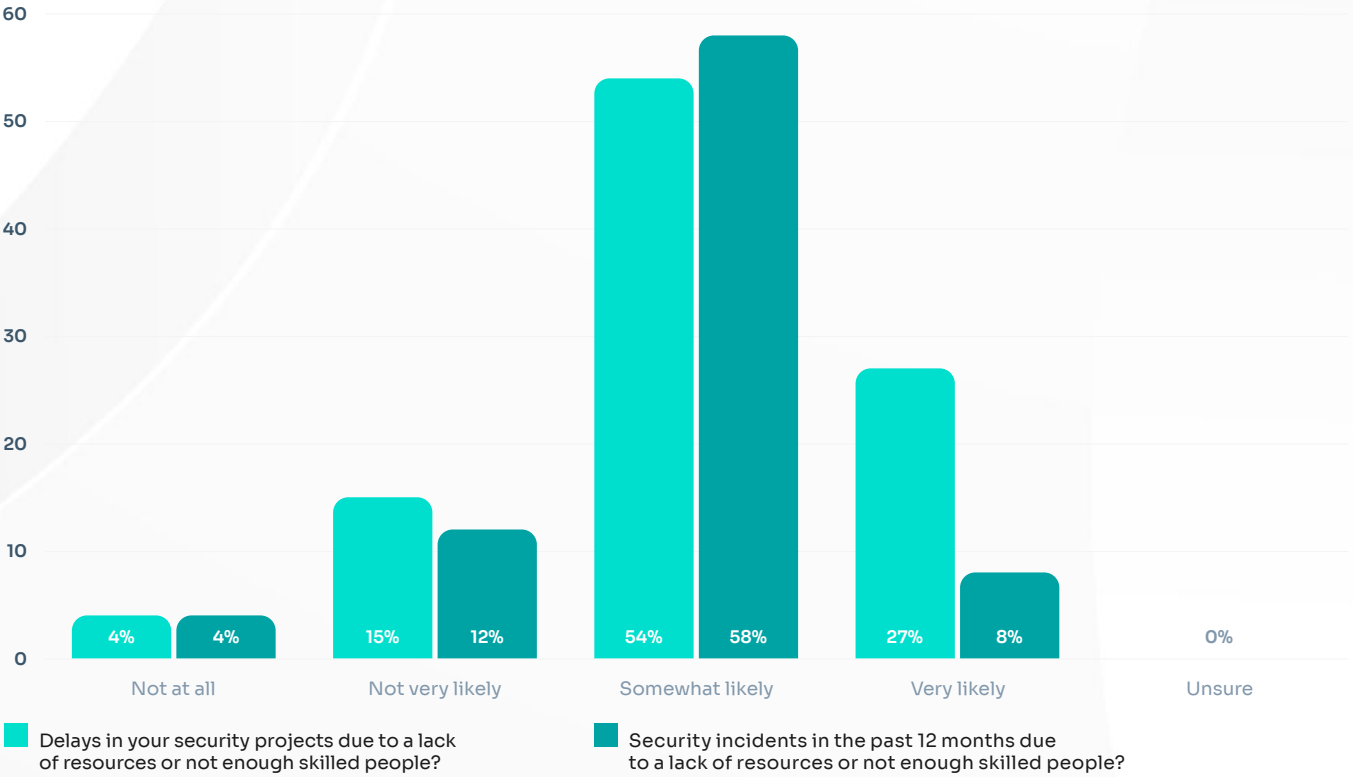
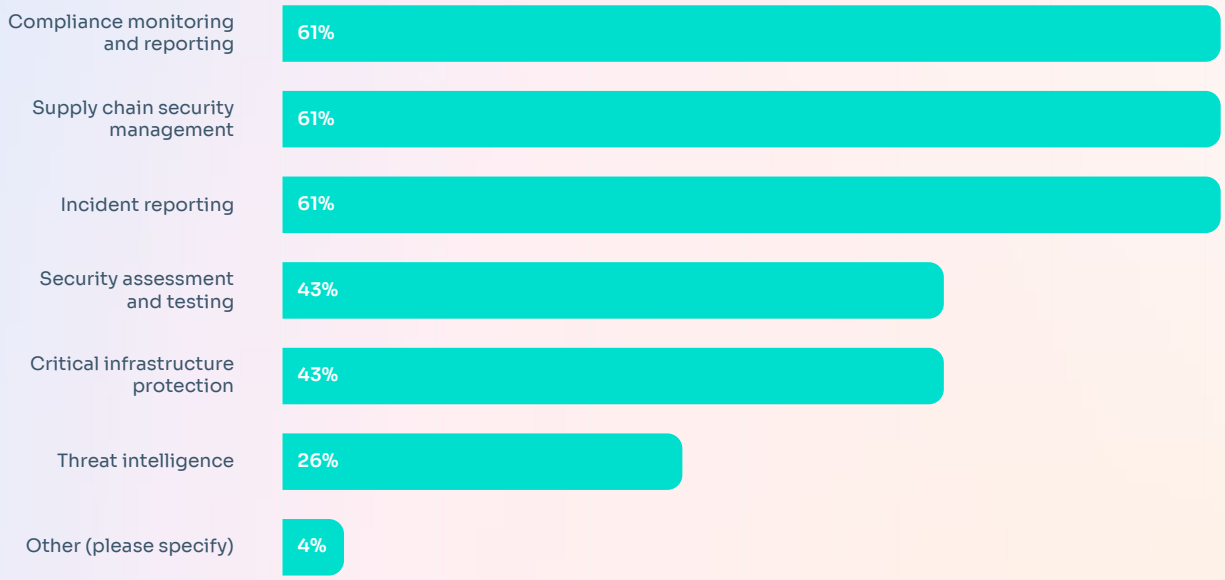
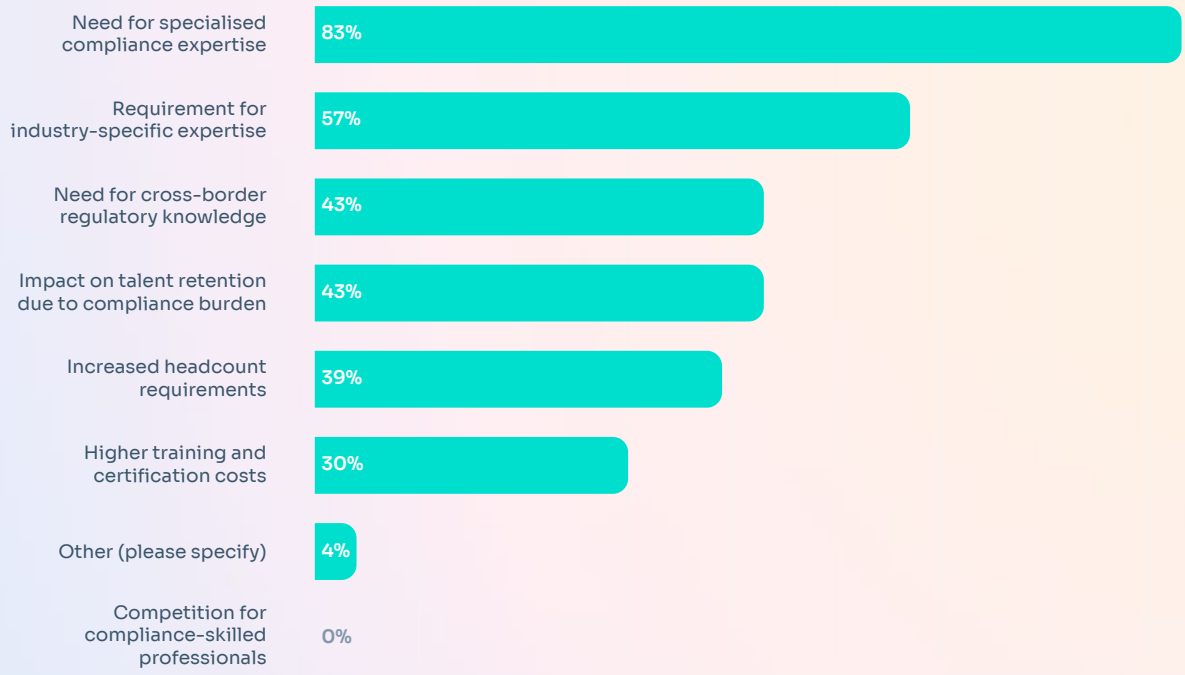


CHART 5: WHICH ASPECTS OF THE NEW CRITICAL INFRASTRUCTURES ORDINANCE CONCERN YOU MOST REGARDING TALENT REQUIREMENTS TO DELIVER?

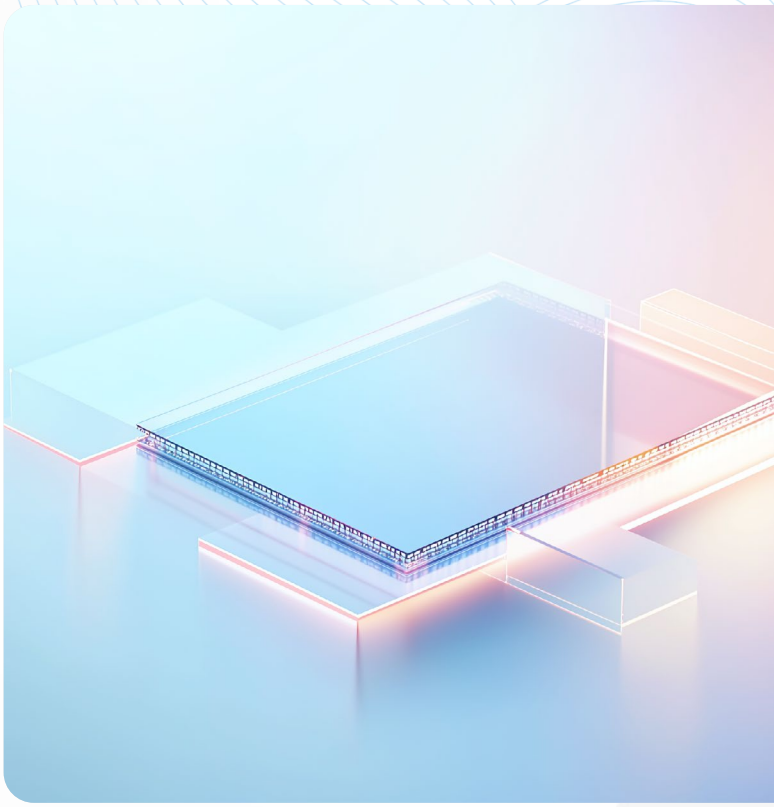


The increasing regulatory requirements are putting considerable pressure on organizations to find the right resources and expand their teams to address these new demands. According to participant feedback, the top three areas of expertise needed are **specialized compliance**, industry-specific knowledge, and cross-border regulatory understanding.

CHART 6: HOW DO REGULATORY REQUIREMENTS AFFECT YOUR CYBERSECURITY TALENT STRATEGY?



When asked, professional recruiters emphasize the **growing importance of cloud security** amid accelerating digital transformation projects. Since the Covid-19 pandemic, the adoption of multi-cloud strategies has significantly increased and consequently the need for professionals with cloud security backgrounds has also grown, which is hard to find.



> There is a growing demand for companies to be hiring for security professionals with the experience of securing cloud environments and managing associated risks on multiple cloud platforms (AWS, Azure, Alibaba). Application security has been one of the niche skill sets in Hong Kong, and as companies migrate their applications to cloud platforms, there is a constant demand for recruiting experts with experience in securing application security across multiple cloud environments."
>
> **Fiona Fung**
> Robert Walters

Similarly, other recruiters have highlighted how digital transformation – fueled by AI, cloud computing, and e-commerce – has increased **reliance on interconnected platforms**, amplifying cyber risks and thus demand for cybersecurity talent.

Regulatory compliance is another common concern. Most headhunters reference the new Critical Infrastructures Ordinance, effective in January 2026, which compels enterprises to strengthen their cybersecurity teams to meet regulatory requirements. This regulatory pressure is driving demand for professionals skilled in risk management, cyber defense, and security architecture.

> [The Critical Infrastructures Ordinance] will increase the demand for cybersecurity talent across risk, cyber defense and security architecture to ensure organizations are able to sufficiently protect their organizations and comply with regulations."
>
> **Elmer Tan**
> EAMES Consulting

In summary, the cybersecurity talent market in Hong Kong is shaped by rapid cloud adoption, digital transformation, emerging AI risks, and tightening regulatory demands.

The experts in the workforce market agree on a **critical shortage of skilled professionals-especially in cloud security, AI security, and operational roles**. These insights portray a competitive and evolving landscape where technical expertise, regulatory knowledge, and adaptability to new technologies are paramount.

How effective is talent acquisition in Hong Kong?

The majority of participants clearly express a **moderate unsatisfaction** when asked about the staff hired in the past 12 months, and only half consider themselves to be satisfied.

CHART 7: HOW SATISFIED ARE YOU WITH YOUR RECENT CYBERSECURITY HIRES WITHIN THE PAST 12 MONTHS?

- 13% Very satisfied
- 35% Moderately satisfied
- 43% Moderately unsatisfied
- 4% Very unsatisfied
- 4% Too early to assess

In more detail, it appears that the reason for such dissatisfaction is in the **gap in terms of technical skills**, followed by poor soft skills and mismatched salary expectations.

Professional recruiters identify critical skill gaps in Hong Kong's cybersecurity workforce as well, though they emphasize different areas. As mentioned, some experts highlight a growing need for hands-on professionals with expertise in cloud security, DevSecOps, cyber threat analysis, and incident response, coupled with a strategic mindset to implement effective security solutions. It is important to notice that the fast evolving of technologies, boosted by AI trend, has definitely contributed to **more stringent requirements from companies**.

CHART 8: IF UNSATISFIED, WHAT ARE THE MAIN REASONS FOR MISMATCHED EXPECTATIONS WHEN RECRUITING CYBERSECURITY TALENT?

Others point to a shortage of candidates with **specific industry and domain knowledge**, especially in regulated sectors like finance, as well as **essential soft skills** such as communication, problem-solving, and collaboration. They also note that practical experience often outweighs certifications alone.

> Employers increasingly value communication, problem-solving, and collaboration skills in cybersecurity professionals, even in non-managerial roles, to facilitate effective engagement with technology teams and business stakeholders. Candidates with cybersecurity certifications but limited hands-on experience from previous roles are often given lower priority by many companies."

Kelvin Chu
Randstad

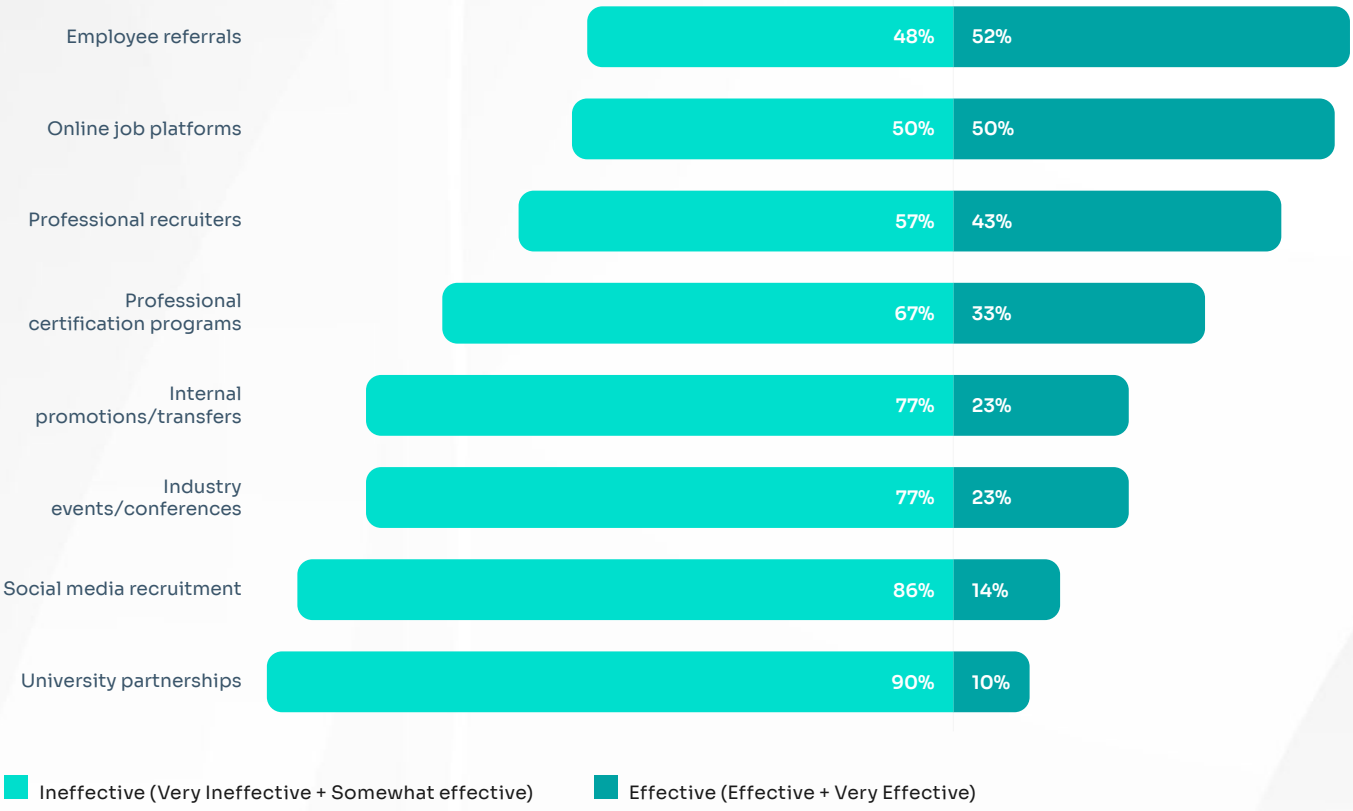
> I concur that, given the evolving landscape of cybersecurity threats and technologies, the requirements for cybersecurity roles have become increasingly sophisticated in order to meet business needs."

Fiona Fung
Robert Walters

In summary, the skills gap in Hong Kong's cybersecurity talent pool spans technical specialties as well as industry-specific knowledge and soft skills necessary for effective cross-team collaboration. This multifaceted gap challenges organizations to find professionals who combine practical experience, strategic thinking, and specialized domain expertise.

When asked about the recruitment strategy and the effectiveness of channels used, **there is not a clear winning approach**. Based on the responses, employee referrals, online job platforms, and professional recruiters are considered the most effective strategies nowadays, while social media and **university partnership** are considered the least effective.

CHART 9: WHICH RECRUITMENT CHANNELS HAVE EFFECTIVELY PROVIDED TOP CYBERSECURITY TALENT?



What are universities doing to support the future cybersecurity talents?

We approached a few universities in Hong Kong to understand the current state of cybersecurity higher education, how future professionals prepare for careers in cybersecurity, and related topics.

A number of universities in Hong Kong offer Information Security or Cybersecurity courses, although the scope and depth vary from institution to institution. Some universities, such as The Hong Kong University of Science and Technology (HKUST), offer **full-time programs** primarily for postgraduate students, with a duration of two years and including advanced subjects such as Cloud Security, Ethical Hacking, and Digital Forensics.

HKUST has recently launched the Msc in Information and Cyber Security Management, a program with 15 courses articulated in 2 years. Approved in January 2025, classes will start in September. According to the HKUST faculty, this program was designed to address the shortage of Cybersecurity talent in Hong Kong and to fill the gap in the academia landscape in Hong Kong.

> “Our research revealed that there are no systematic courses in cybersecurity management across Hong Kong universities. While computer science programs exist, there is a lack of dedicated cybersecurity management programs. HKUST has a few undergraduate courses aligned with CISA certification, and this new master’s program aims to elevate the curriculum by focusing not only on technology but also on human factors and policy.”
>
> **Prof. Weiyin Hong**
> HKUST

HKUST puts significant **effort into balancing theoretical courses with practical experience and establishing connections with the professional world**. For instance, the university has formed partnerships and collaborative initiatives with the banking industry, particularly with the Hong Kong Monetary Authority (HKMA) for applied cybersecurity research, and with the Hong Kong Institute of Bankers (HKIB) to develop a professional certificate program for banking professionals. Additionally, HKUST has long-term relationships with the international professional association ISACA, which supports students in preparing for cybersecurity certifications by providing discounts on exam fees and reducing experience requirements. Furthermore, the university regularly involves external professionals in its courses to ensure that students benefit from real-world experience and the most up-to-date practices.

> “Roughly half of our faculty members are practitioners from industry (e.g., incident response, risk management, digital forensics, cloud computing security) and include senior engineers and information security managers from companies like Google, Welab, and AWS. This ensures that students gain practical insights from experts in the field [...] We collaborate with local companies to facilitate capstone projects and internships.”

Prof. Weiyin Hong
HKUST

Keeping the courses and curriculum up to date is one of the key challenges highlighted by HKUST faculty members. The rapid pace of change in technology and cybersecurity necessitates annual updates to course content. Therefore, the involvement of practitioners is fundamental to address this gap.

Another challenge is to encourage students from diverse backgrounds to take an interest in information and cybersecurity. These subjects have **traditionally been part of computer science programs, focusing primarily on hard technical skills,** which has limited participation from non-technical students. However, information security encompasses topics such as regulation, compliance, privacy protection, IT auditing, and risk management, along with essential soft skills like management and communication.

For the future, HKUST stresses the importance to provide a well-balanced curriculum of hard and soft skills, to strengthen the relationship with experienced practitioners, and to provide internationally recognized certifications.

> “We recognize our areas for improvement and actively incorporate industry experts into our programs. By aligning our offerings with professional certifications like CISA and CISM, we focus on broader, in-demand skills relevant to the Hong Kong market..”

Prof. Weiyin Hong
HKUST

Other universities offer courses, generally for one semester, which can be part of either graduate or postgraduate programs. The Hong Kong Shue Yan University (HKSYU) offers a **cybersecurity course for one semester** as part of the Financial Technology Program. This course is a simplified version of the CISSP curriculum, as covering the full curriculum would require more time. The course includes contributions from cybersecurity practitioners, as well as demonstrations of tools currently used in the market.

According to Bosco Tsin, a lecturer in the Department of Economics and Finance, several improvements are already under discussion to expand the course and better align it with the local market.

“

We suggest including more insights about the current cybersecurity and data protection laws in Mainland China. Since the CISSP framework is based on an American context, we believe it is important to also focus on local regulations and standards.

Additionally [...] we aim to extend the course for another semester and combine it with other practices, such as the Software Development Life Cycle, to illustrate how security is integrated. The key objective is to make the content less abstract and encourage students to consider the broader picture.”

Bosco Tsin
HKSYU

The university also wishes to strengthen its relationship with the cybersecurity industry, particularly by **establishing solid partnerships with companies** to introduce group projects and internship initiatives during postgraduate courses. However, it appears that companies in Hong Kong are not very receptive to strengthening these relationships. According to Mr. Tsin, the challenges stem from cultural factors and the perception of mismatched expectations regarding the value that students can bring.

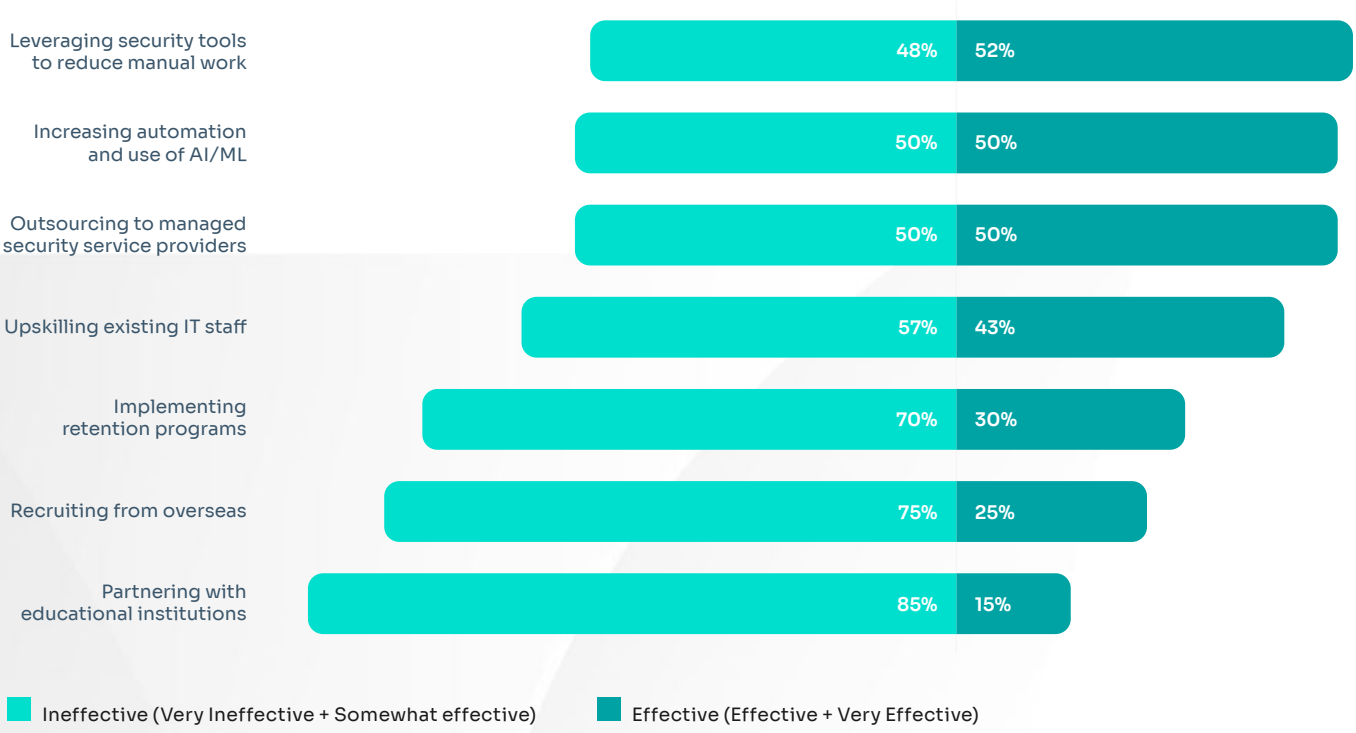
What are organizations doing to face the current challenges?

Considering the widely recognized shortage of cybersecurity talent, we asked organizations what strategies they have deployed to address this challenge. Most organizations are tackling this issue by **increasing automation and use of AI and Machine Learning**. Additionally, upskilling the existing IT staff through dedicated training programs, along with outsourcing to managed service providers, are the most used strategies.

When asked about the effectiveness of these strategies, outsourcing and automation were deemed very effective compared to the others. Partnering with educational institutions was again considered the least effective.

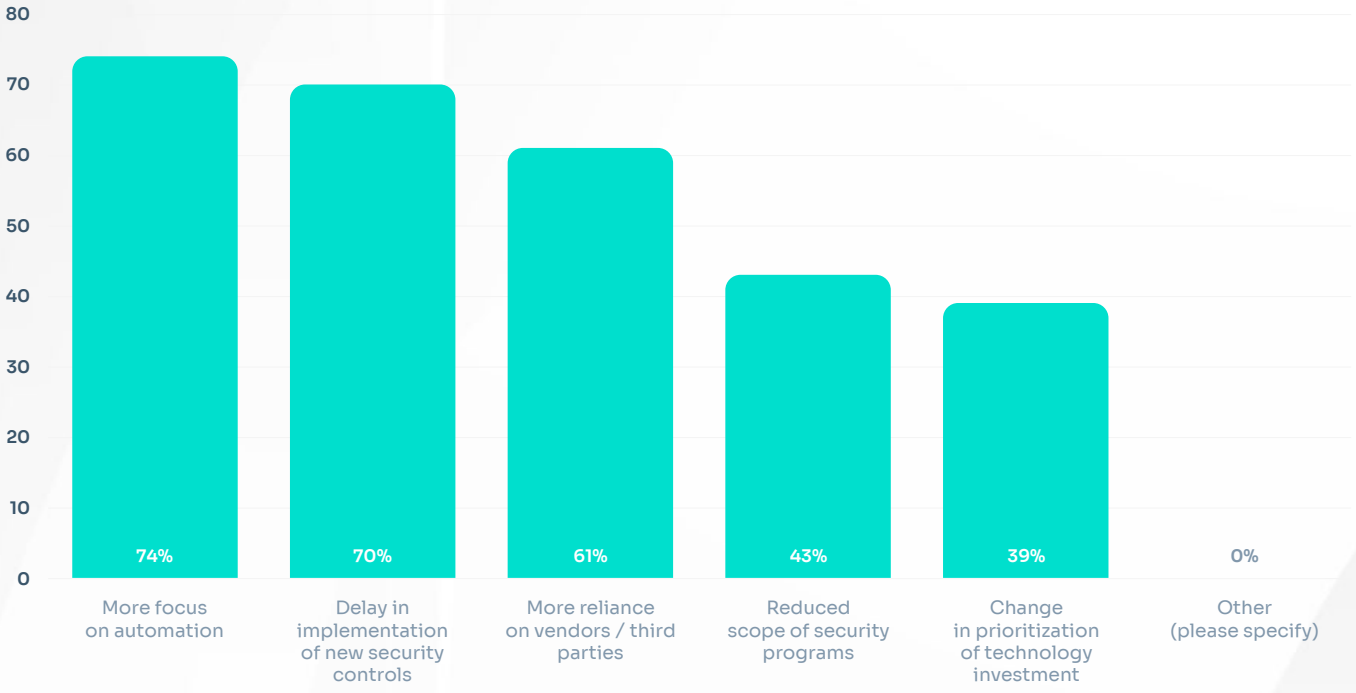
CHART 10: WHICH STRATEGIES ARE CURRENTLY BEING DEPLOYED BY YOUR ORGANIZATION TO ADDRESS THE TALENT SHORTAGE?

CHART 11: HOW EFFECTIVE HAVE THESE STRATEGIES BEEN TO ADDRESS THE TALENT SHORTAGE?



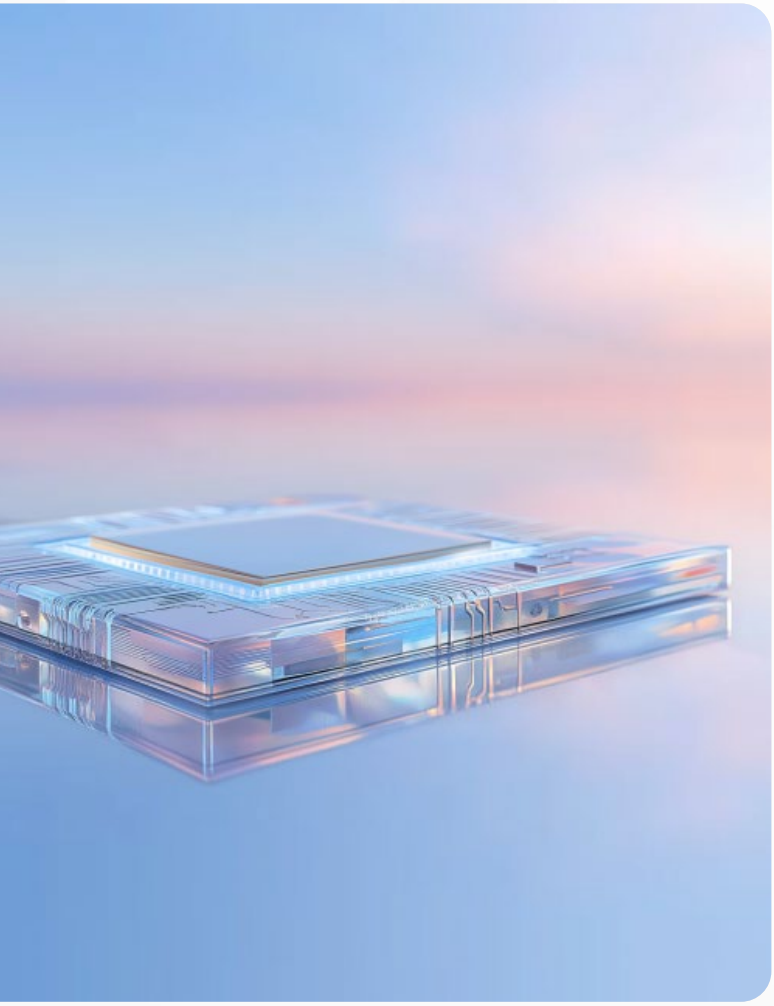
This aligns with the responses from most participants, who indicated the **utilization of security tools**, a greater reliance on **third-party vendors and an increased automation and use of AI / ML** as response to the talent shortage's impact on their security strategies. However, on the negative side, this shift has not eliminated delays in implementing new security controls or in reducing the scope of security programs.

CHART 12: HOW HAS THE TALENT SHORTAGE INFLUENCED YOUR SECURITY STRATEGY?



Most professional recruiters agree with the current strategies that companies are adopting to address talent shortages and economic factors. However, they shared some caution against **over-reliance on candidates' experience** and emphasized the importance of training and upskilling programs.

> Focusing too heavily on experience rather than skills, certifications, or potential, companies may be overlooking capable candidates who could grow into the role with proper training and mentorship."
>
> **Jacky Chow**
> Hays



Furthermore, recruiters have noted a growing trend of outsourcing resources to professional service providers across Southeast Asia, enabling organizations to access skilled personnel at a lower cost, while adhering to ongoing budget constraints across all departments, not just Cybersecurity. Cross-border recruitment has also been highlighted, particularly from **Mainland China**, especially for mid- to senior-level roles. However, there are challenges in persuading senior professionals to relocate to Hong Kong.

> "To address the talent shortage, outsourcing has become a common practice for specific roles. However, outsourcing should be balanced with the development of the internal workforce. For multinational companies, a best practice is to establish internal service centers in countries where it is easier and more cost-effective to access skilled staff, such as Mainland China. Companies often set up a Center of Excellence (CoE) at the group level to serve various markets across their footprint. CoEs ensure that these markets adopt the right standards, policies, and the latest technology."
>
> **Silvia Ihensekhien**
> Swire Coca Cola

What are the salary expectations?

As previously mentioned, one of the top 3 gaps identified is mismatched salary expectations. Digging more on this specific matter, it appears that hiring cybersecurity talent necessitates a salary increase. Almost half of the responses indicate a need for a salary increase of up to 10% compared to the candidate's current salary. In some isolated cases, the increase may reach as high as 30%, depending on the role.

CHART 13: WHAT % INCREASE IN SALARY OFFERS HAS BEEN NEEDED TO HIRE CYBERSECURITY TALENT IN THE LAST 12 MONTHS?

48% responses
Less than 10% increase

39% responses
Between 11% and 20% increase

13% responses
Between 21% and 30% increase

According to professional recruiters, candidates in Hong Kong's cybersecurity market generally expect salary increases of around 15-20% when changing jobs, though some **may accept as low as 10%** depending on their circumstances. Junior to mid-level professionals typically seek this range, while senior candidates might accept smaller increases if offered long-term stability and growth opportunities.

Based on the survey's responses, most organizations consider their compensation packages **slightly above average or on market average**.

CHART 14: HOW COMPETITIVE DO YOU CONSIDER YOUR CYBERSECURITY COMPENSATION PACKAGES COMPARED TO THE HONG KONG MARKET?

4% Highly competitive (top quartile)

35% Moderately competitive (above average)

35% Market average

17% Below market average

9% Varies by role

However, some companies, especially smaller firms or those with tight budgets, **struggle to meet these expectations**, leading to challenges in attracting and retaining talent.

Professional recruiters align closely with feedback from the professional community. Most headhunters agree that junior to mid-level candidates typically expect a **15-20% salary increase**, while senior professionals may prioritize stability over salary growth. Below market offers, especially for junior roles, create mismatches between candidate expectations and employer offerings, complicating recruitment and leading to prolonged vacancies.

On one hand, candidates are aware of the talent shortage and generally do not lower their salary demands, particularly at junior and mid-levels where salary growth is most rapid. On the other hand, recruiters acknowledge that **salary increments have decreased**, reflecting budget constraints, especially among small to medium-sized companies.

“Despite a general trend of IT candidates seeking less aggressive salary increments due to the current market, most still anticipate a 15-25% salary increment when changing roles. Some companies, particularly smaller ones or those with tighter budgets, may find it challenging to meet these expectations.”

Kelvin Chu
Randstad

In summary, candidate salary expectations in Hong Kong’s cybersecurity sector remain robust, generally seeking 15-25% increases upon job changes. However, some employers’ reluctance or inability to match market rates-especially at junior levels-creates hiring challenges. The competitive market and talent shortage empower candidates to maintain higher salary demands, contributing to ongoing recruitment difficulties for companies offering below-market compensation.

What motivates candidates to have a cybersecurity career?

Most recruiters in Hong Kong agree that **job stability has become a top priority** for cybersecurity candidates, especially amid economic uncertainty. Therefore, there seems to be a shift a few years ago, where candidates were seeking large salary increases at multinational firms, preferring stable local enterprises and financially sound employers. Cybersecurity is widely considered as a stable, well-paying field that is intellectually stimulating due to increasing AI exposure and evolving threats.

For this reason, there is a growing trend of people within the IT domain to look to **move into cybersecurity roles**, which gives more stability and potentially higher salaries, although this might represent more challenging roles.

“It is common to see candidates in the IT space, whether in applications or IT infrastructure, looking to move into cybersecurity roles as salaries are usually higher in this space.”

Elmer Tan
Eames Consulting.

Retention of cybersecurity talent represents a key challenge for companies today. According to most participants, cybersecurity roles are becoming increasingly demanding, leading to higher risks of fatigue and burnout. Companies need to consider **additional benefits beyond competitive salary packages**, such as avoiding long working hours and ensuring a healthy work-life balance. Furthermore, investing in internal cybersecurity resources is critical to encouraging professionals to stay longer within the company. In a highly competitive market, talent is constantly approached with new opportunities and potentially better offers.

“Retaining talent would be more achievable when companies provide on-the-job training, allow candidates to rotate through their job responsibilities, enable them to acquire new skill sets, and offer sponsorship for obtaining new cybersecurity certifications.”

Fiona Fung
Robert Walters.

“

The cybersecurity workforce market is particularly challenging today. To attract and retain top talent, companies must invest in their resources. Improving training practices is fundamental, and organizations should focus on upskilling their current staff. Human Resources departments should provide guidance on training opportunities. In addition to competitive salaries, companies should also offer extra benefits. Since cybersecurity is considered a demanding and stressful field, organizations must ensure their staff maintain a healthy work-life balance.”

Silvia Ihensekhien
Swire Coca Cola

“

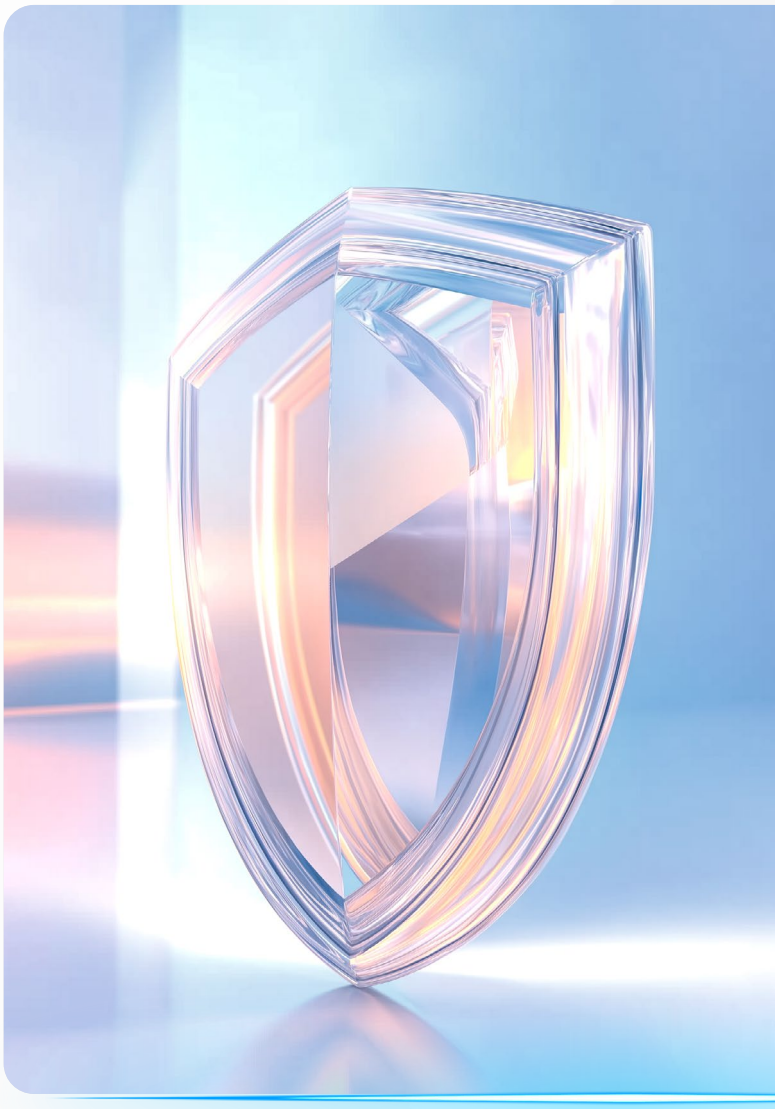
Regarding the job market in Hong Kong, there is no easy fix. In addition to nurturing and supporting the local professional community, Hong Kong needs to offer substantial opportunities for professionals from abroad to pursue and advance their careers. Building a strong culture of cybersecurity professionals within the community will require a long-term strategy.”

Frankie Tam
Eversheds Sutherland

“

Organization leaders should treasure and appreciate the hard work of cybersecurity professionals, while cybersecurity professionals should uphold a high standard of professionalism. The CFOs of organizations should not measure the cybersecurity team's effort only by ROI, while cybersecurity professionals should demonstrate their value."

Wilson Tang
HKCNSA



How much are companies investing in cybersecurity?

According to market research, Cybersecurity budgets in the Asia-Pacific (APAC) region are **growing robustly**, with spending projected to reach USD 12 billion by 2027, driven by a compound annual growth rate (CAGR) of 12-13%[8]. This is mainly due to the intensification and sophistications of cyber threats, including a continuous rise in ransomware attacks, pushing enterprises of all sizes to prioritize cybersecurity investments.

Based on the survey, most companies **allocated between 5% and 10% of their IT budget to cybersecurity in 2024**. This is generally in line with global benchmarks, which have recently indicated an average allocation of 5.7% of annual IT spending[9]. The allocation of the cybersecurity budget has been a subject of much debate among researchers and subject matter experts, who argue that it can be a misleading indicator and does not provide a solid assessment of the state of security[10]. However, the cybersecurity community increasingly agrees that budgets for cybersecurity should rise in the future due to more frequent and sophisticated attacks and growing regulatory requirements. Despite this, more than half of the participants **expect their budgets to remain stable for 2025**, while others anticipate a decrease.

> While cybersecurity remains a key priority, economic downturns can lead to budget constraints in some organizations, potentially slowing down hiring or limiting their ability to meet high salary expectations. Nevertheless, even with increased caution in hiring, cybersecurity budgets have generally not experienced significant cuts compared to other areas."

Kelvin Chu
Randstad

When asked about budget allocation to talent acquisition and retention within the Cybersecurity department, most participants claim that they invest up to 25% on this activity.

CHART 15: IN TERMS OF IT BUDGET, HOW MUCH BUDGET HAS BEEN ALLOCATED TO CYBERSECURITY FOR 2025?

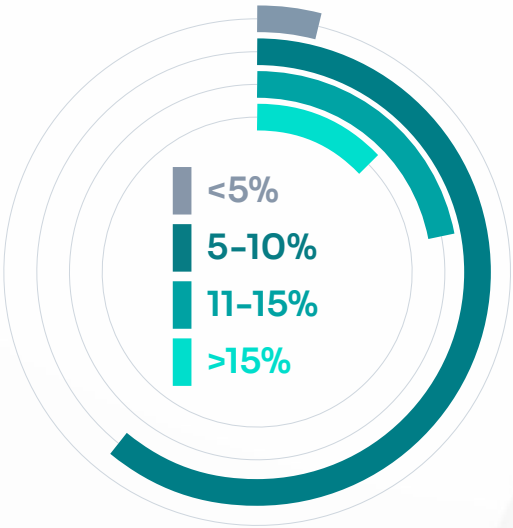
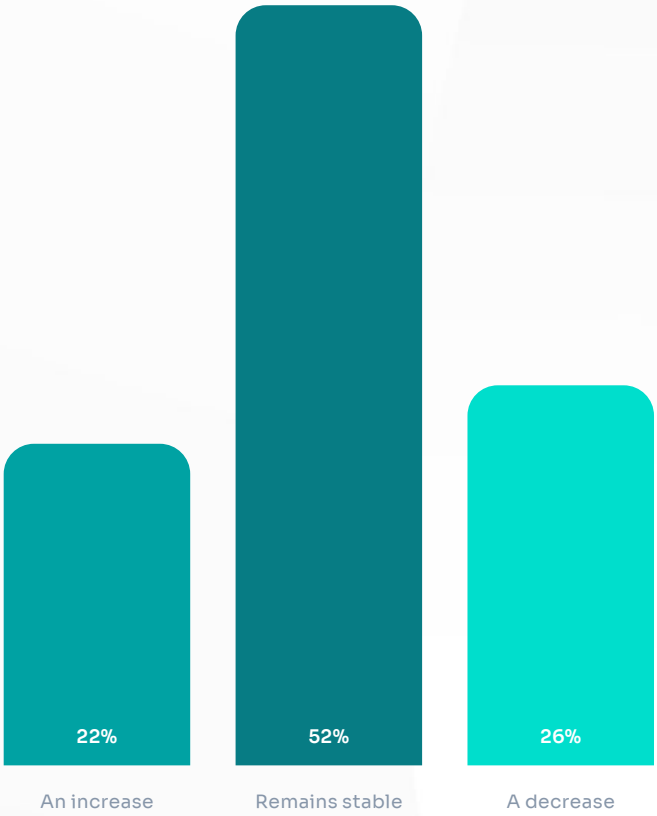


CHART 16: BASED ON THE CYBERSECURITY BUDGET OF 2024, HOW DOES THE 2025 ALLOCATION COMPARE?



(8) IDC Playbook for Tech Marketing Leaders: Capitalizing on SMB and Midmarket Security Spending for Growth in Asia/Pacific, October 2024
(9) Forrester's 2024 Cybersecurity Benchmarks Global Report
(10) Identifying the Real Information Security Budget, Gartner, August 2016

Are there unique challenges for cybersecurity talent in Hong Kong?

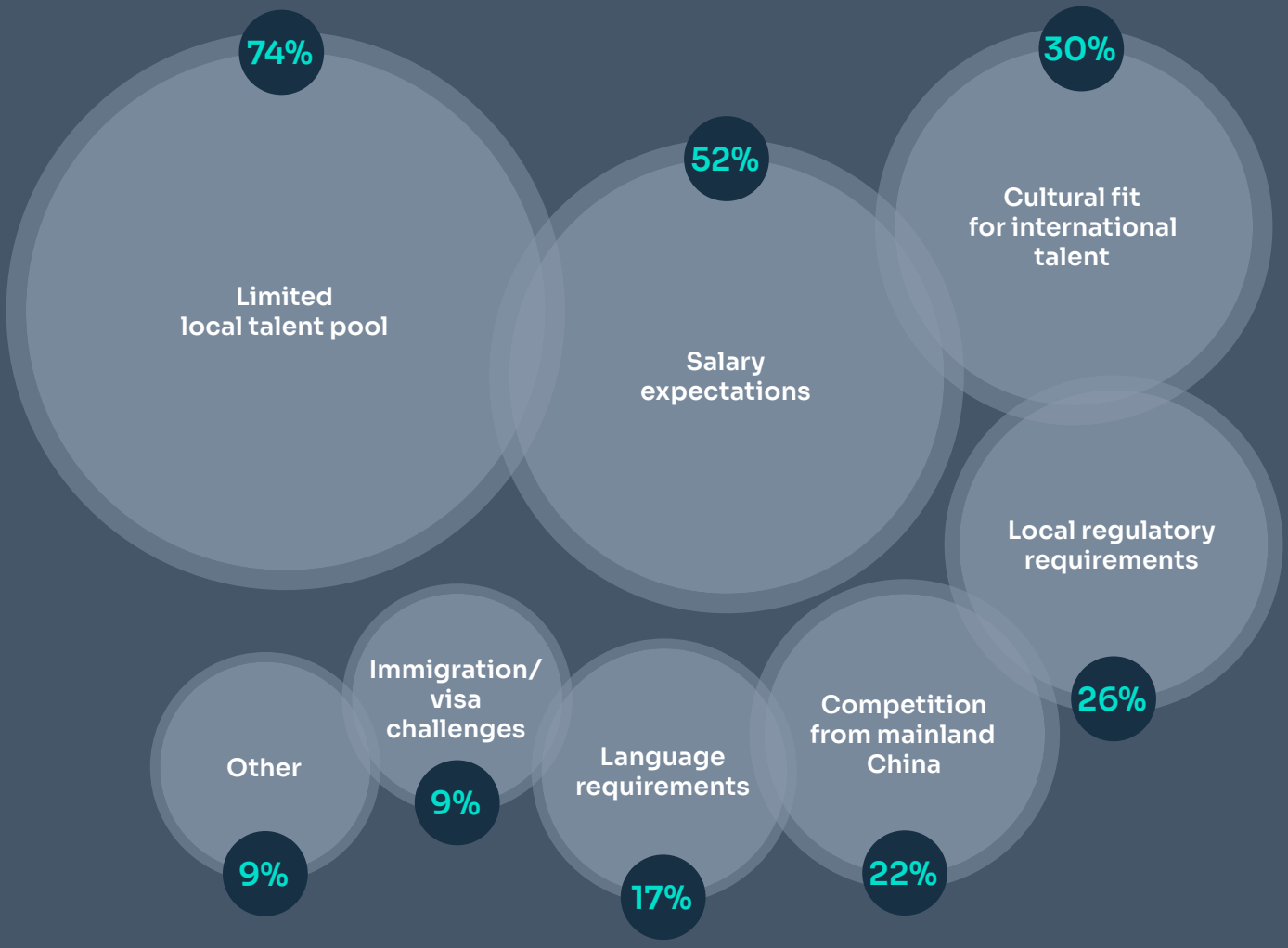
When reviewing the responses from participants and examining the situation in Hong Kong, it's natural to wonder whether the region has unique conditions that make the cybersecurity recruiting market particularly challenging.

Participants expressed a strong belief that the main issues stem from a **limited local talent pool and high salary expectations**. They also indicated that other countries in the Asia Pacific region face similar challenges, though some believe the situation is more severe in Hong Kong.

The actual figures regarding workforce trends seem to validate the participants' opinions. Between 2020 and 2022, the labor force in Hong Kong shrank by approximately 140,000 individuals[11]. This phenomenon has been termed "brain drain" as it primarily affected skilled workers. In contrast, Singapore demonstrated greater resilience during the same period. Although net migration showed a significant decline, it remained positive and recovered to pre-pandemic levels by 2022[12].

According to the Hong Kong Talent Engage office (HKTE), **potential overseas talents lack understanding of Hong Kong's industry landscape**, career pathways, and the talent attraction measures implemented by the Hong Kong Government. This issue also extends to talent from Mainland China. Although they may be more familiar with Hong Kong, they still encounter cultural differences and have limited proficiency in English and Cantonese, making their adaptation to both professional and personal life more challenging.

CHART 17: WHAT UNIQUE CHALLENGES DO YOU FEEL ARE SPECIFIC TO HONG KONG REGARDING CYBERSECURITY TALENT?



(11) "Brain Drain and Brain Gain in Hong Kong's Population Shuffle", Migration Policy Institute, April 2024
(12) Singapore Net Migration 1960-2025, Macrotrends

> The prevalent perception of Hong Kong's high living costs, alongside its elevated living standards, often dampens their interest in relocating."
>
> **Anthony Lau**
> Hong Kong Talent Engage

To counter the outflow, Hong Kong implemented several measures, notably the **Top Talent Pass Scheme (TTPS)** in late 2022, which attracted around 90,000 people to Hong Kong over the next two years, with a significant majority coming from Mainland China[13].

In this perspective, it is also important to highlight the **corporate relocation of headquarters to Singapore**. According to intelligence data from 2023, Singapore has taken a dominant position compared to Hong Kong, with major companies establishing their regional headquarters there, including Google, Microsoft, FedEx, Rolls Royce, and other multinational firms[14].

In the recently approved **Hong Kong Budget for 2025-2026**, the Hong Kong Government has reinforced several initiatives aimed at increa-sing market competitiveness, attracting foreign companies and talent, and supporting local bu-sinesses. In particular, these initiatives include tax support measures, changes to immigration po-licies, a HK$1.5 billion Research Matching Grant Scheme, and HK$1 billion allocated to establish an AI research and development institute, among others[15].

(13) Hong Kong Free Press, February 2025
(14) "Multinationals Pick Singapore Over Hong Kong for Asian Headquarters", Bloomberg, February 2024
(15) Budget.gov.hk

3. Looking at other countries in Asia: the case of Singapore

It is worth taking a brief look at other countries in the region, particularly Singapore, which also seems to be experiencing similar challenges regarding the cybersecurity workforce.

Singapore's cybersecurity workforce has experienced a significant growth in the past. According to a recent study, from 2016 to 2022, the number of professionals has tripled, reaching 12,000 individuals, with a market size of about SGD 2 billion.

As for other leading Asian hubs, emerging technologies like generative AI and quantum computing are introducing new vulnerabilities, intensifying cyber threats and driving demand for advanced cybersecurity measures. Despite this expansion, Singapore also faces a significant talent shortage, with demand outpacing supply and creating a skills gap.

According to local professional recruiters, at the moment there is a **high-demand roles such as Security Architects, Security Operations Specialists, Digital Forensics Experts, Penetration Testers, and Cloud Security Engineers**. The job market is shaped by rapid technological advances and strict regulatory requirements, with employers prioritizing hands-on experience over certifications.

Economic uncertainties and geopolitical tensions have heightened threats, especially to critical infrastructure and Ope-

rational Technology environments. While overall job growth has slowed, cybersecurity hiring remains resilient due to evolving threats and regulations.

> Stringent experience and certification requirements limit opportunities for junior professionals and fresh graduates. This barrier makes it challenging for entry-level talent to break into the field, contributing to the talent shortage and increasing turnover as junior professionals seek roles better aligned with their career goals."
>
> **Isha Hussain**
> Robert Walters

Compensation expectations average a **15% salary increase** when changing jobs, often exceeding what companies offer, leading to mismatches. Retaining talent is challenging amid fierce competition and the need for continuous learning, which can cause stress and burnout.

Looking ahead, Singapore cybersecurity demand is expected to grow significantly over the next 3-5 years, pushed by regulatory requirements, continuous digital transformation projects as well as increasing cyber-attacks.

> The cybersecurity market in Singapore is expected to reach USD 2.65 billion by 2025, with a compound annual growth rate (CAGR) of 16% through 2030."
>
> **Isha Hussain**
> Robert Walters

The **Cyber Security Agency of Singapore** (CSA), the government agency that provides centralized oversight of national cyber security functions and aims to protect Singapore's Critical Information Infrastructure (CII), is planning to invest S$50 million to uplift Singapore's cybersecurity sector, as part of the **three-year Cybersecurity Talent, Innovation & Growth (Cyber TIG) Plan**[16]. Unveiled in September 2023, the Cyber TIG Plan is a joint initiative between the Cyber Security Agency of Singapore (CSA) and the National University of Singapore (NUS) with the aim to establish the nation as a global cybersecurity innovation hub by integrating talent development, startup acceleration, and industry growth through three pillars[17]:

- 1. **Talent:** training non-cyber professionals via programs like SG Cyber Associates and nurturing youth through SG Cyber Youth;
- 2. **Innovation:** supporting startups via CyberBoost and AI / Quantum research; and
- 3. **Growth:** expanding local cybersecurity firms internationally through CyberGrowth.

Backed by S$20 million in government-NUS funding, the initiative unites academia, industry, and government to address talent gaps and drive scalable solutions.

Among other collaborations between the Ministry of Education and the Cyber Security Agency (CSA), there is the"SkillsFuture" initiative, launched in 2015. This program, in collaboration with NUS, offers cybersecurity education and funds up to 90% of course fees for individuals, benefiting both citizens and local private companies[18].

> "In Singapore, professionals have the opportunity to join programs like the Technology Finance Immersion Program (TFIP), and to attend industry-curated structured trainings, followed by attachment with financial institutions to gain on-the-job experience to pivot into a career in technology within the Financial Services sector."
>
> **Elmer Tan**
> Eames Consulting

16 Cyber Security Agency of Singapore (CSA), Press Releases, September 2023
17 Cyber Security Agency of Singapore (CSA), Press Releases, July 2024
18 SkillsFuture, Mid-Career Enhanced Subsidy

4. What's next: Conclusions and Future Outlook

Key considerations

Hong Kong's cybersecurity challenges stem from a mix of workforce deficiencies, including gaps in both technical skills and soft skills, as well as high salary expectations. The strategies implemented so far to address these gaps have not yielded the expected benefits. As a result, the gaps persist, impacting the capacity to deliver security projects and activities.

Understanding the root causes of these gaps is not straightforward. Some professional recruiters believe that **the reasons are systemic**, and the unique context of Hong Kong has not facilitated resolution. The resulting talent shortage has driven up hiring costs, prompting companies to **seek more automation and outsourced services**, particularly from locations outside Hong Kong where services can be provided remotely and labor is cheaper (e.g., India, Malaysia, Philippines). Additionally, attracting talent to relocate to Hong Kong has proven difficult due to a combination of visa sponsorship issues, relocation complications, and salary expectations.

We asked participants which initiatives would be most effective in addressing the talent shortage challenges in Hong Kong, and the feedback was quite mixed. Most respondents believe that

professional certifications, training initiatives and **partnerships with academia** would be effective. Others are convinced that talent development initiatives and government support programs would yield better results.

“

Today, new technologies and solutions are being introduced at an unprecedented pace. In this context, it is crucial for professionals to update their knowledge and skills more frequently than before. The traditional model of long classes, sometimes lasting several days and occurring only once a year or every few years, is no longer suitable or sustainable.

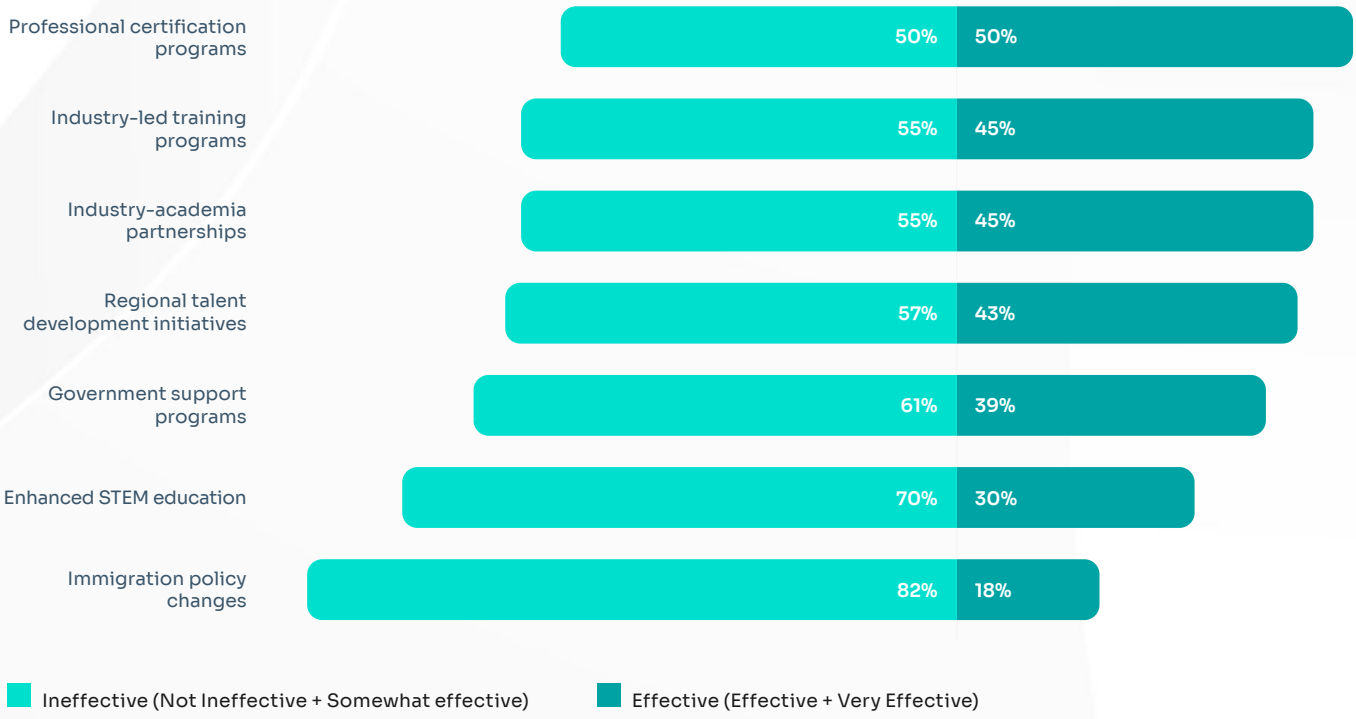
To address the technical skills gap, organizations need to adopt more flexible and streamlined learning frameworks. Professionals should have access to regular and shorter training modules that still lead to certified training.

While there are plenty of training programs available online, individuals need proper guidance to navigate these options. The abundance of online education can make it challenging to choose the right courses.

Universities can certainly help in this matter, but they must be agile in developing and delivering courses. Given the fast pace of technological change, courses may already be outdated by the time they are released.”

Frankie Tam
Eversheds Sutherland

CHART 18: IN YOUR OPINION. WHAT INITIATIVES WOULD BE MOST EFFECTIVE AT ADDRESSING THE CYBERSECURITY TALENT SHORTAGE IN HONG KONG?



“

Increased collaboration across industries is essential. Sharing best practices and discussing challenges will strengthen the cybersecurity community. Enhanced communication and knowledge sharing will enable professionals to learn from one another.”

Silvia Ihensekhien
Swire Coca Cola

This aligns with the strategy and initiatives of the Hong Kong Talent Engage office (HKTE), which aims to **strengthen collaboration with industry associations** and enhance on-the-ground support for incoming talents by assisting professionals and their families throughout the settlement process.

“

The key to attracting I&T and cybersecurity talent lies in effectively showcasing industry prospects and opportunities in Hong Kong. To this end, HKTE will intensify its efforts to highlight these through outreach programmes and online promotion on social media platforms.

HKTE will also collaborate with industry associations to organize targeted recruitment campaigns overseas, similar to the GBA Talent Development Showcase in Kuala Lumpur this April [...] where HKTE led a delegation of nearly 40 leading enterprises in the Greater Bay Area (GBA) and hosted a showcase to directly engage with local talent.”

Anthony Lau
Hong Kong Talent Engage

The demand for cybersecurity professionals in Hong Kong is expected to grow steadily over the next 3 to 5 years. Some recruiters note that **persistent cyber threats will maintain steady demand, particularly among local and Chinese companies**, even as some multinationals relocate roles elsewhere. Additionally, this growth will be supported by ongoing digital expansion and increased awareness of data protection.

In general, there will be a rising demand for skills in cloud security, AI security, and incident response as Hong Kong strengthens its position as a regional financial and tech hub, while generalist roles may decline due to automation. Regulatory changes will also drive hiring in risk and compliance roles.

“

Generalist roles will continue to phase out as automation and AI take over mundane tasks, whilst the focus shifts towards candidates who are highly technical and adaptable in a rapidly changing technological and cyber threat landscape.”

Elmer Tan
Eames Consulting

In summary, cybersecurity demand in Hong Kong will continue to rise, focusing on advanced technical skills, adaptability, and regulatory compliance.

Recommendations for the Future

At the end of the survey, we asked participants a few open questions about how to address the current talent shortage through innovation and what the government and industry bodies could do to improve the situation. We also inquired about how they see the situation evolving in the next 3 to 5 years.

When asked about innovative approaches to address the cybersecurity talent shortage, the vast majority pointed to **new AI-powered tools, particularly mentioning AI for SOC and AISecOps**. Some participants also suggested setting up overseas and offshore centers of excellence, specifically in Mainland China and Malaysia, where labor costs are lower.

We also sought recommendations for the government and industry bodies to address the current shortage. Participants encouraged **strengthening industry-academic partnerships**, including the promotion of industry-specific certifications by the government. Additionally, they advocated for more dedicated cybersecurity programs and degrees at universities, rather than just isolated classes. This should be accompanied by greater career guidance and work experience sharing to assist young graduates in their career choices.

HKTE has already taken action in this direction by building a solid network with top universities, in order to promote the latest updates about Hong Kong's talent admission policies.

> During its global promotion campaigns, HKTE has successfully built a networking community with world's top 100 universities as well as representatives from industry associations and organizations worldwide. This network serves as an ongoing channel to disseminate the latest updates about Hong Kong's development and talent admission policies to global professionals.

> Locally, HKTE proactively engages with universities across Hong Kong to encourage non-local students to consider remaining in the city after graduation, highlighting the career opportunities available"

Anthony Lau
Hong Kong Talent Engage

Regarding the future, most participants agreed that **the talent shortage will persist**, if not increase, and that actions must be taken to address it. Otherwise, it will increasingly impact Hong Kong's competitiveness and digital leadership in the region.

> HK will be losing out in the long term if not having locally trained talents."

Survey participant

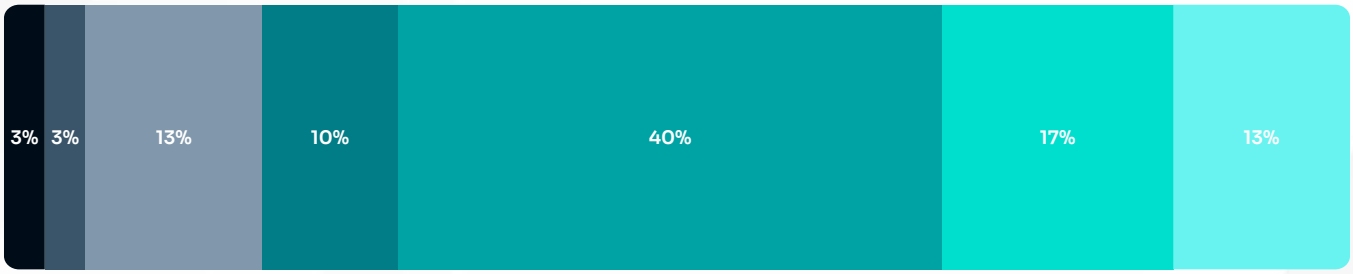
> Through support from government initiatives and modification to education curriculum, we will see more home grown talent."

Survey participant

While AI-driven solutions will definitely help optimize tasks, automate processes, and combat AI-based cyber attacks, long-term initiatives supported by government and academia will be crucial in building a solid backbone of talent and highly skilled professionals, both locally and by attracting individuals from other countries.

Appendix

Survey Participants by Industry



Manufacturing & Industrial Production

Construction & Infrastructure

Technology & Telecommunications

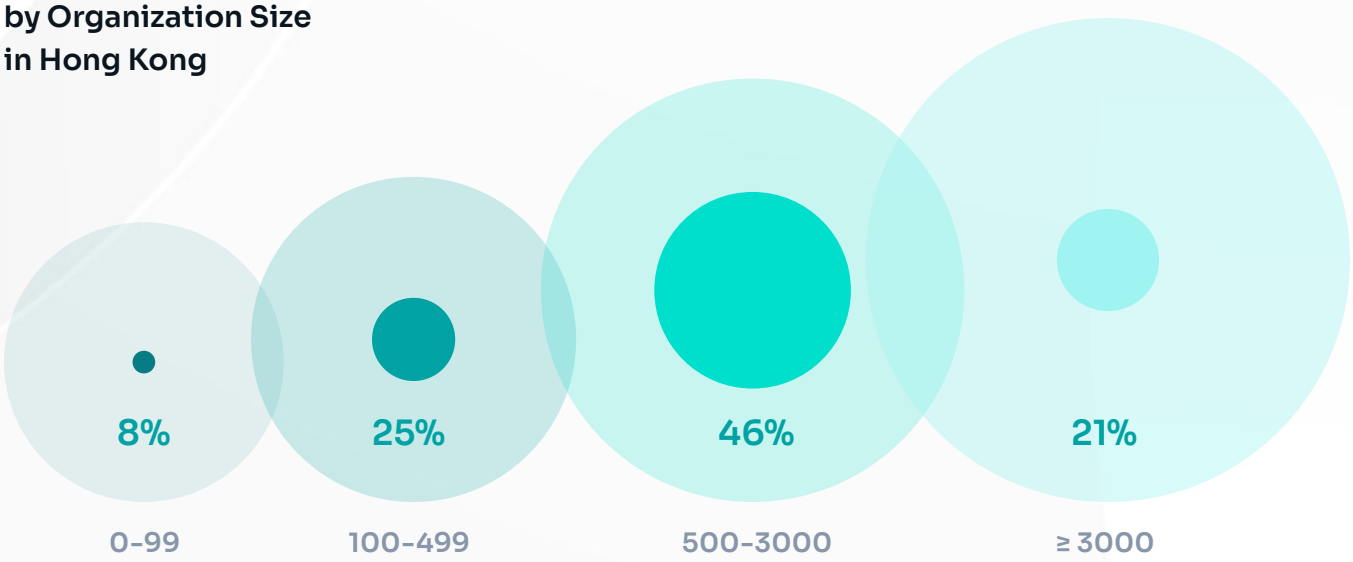
Transports & Logistics

Financial Services & Insurance

Education & Research

Other

Survey Participants by Organization Size in Hong Kong



/ Your contact

Jolly Liang

Marketing & PR Manager

HKCNSA

jolly.liang@hkcnsa.org

Stefano Fois

Senior Industry Expert

Digital & Technology Transformation

Hong Kong

stefano.fois@sia-partners.com

Amaya Rousseau

Manager

Cybersecurity, Data Protection & IT Risks

Hong Kong

amaya.rousseau@sia-partners.com

SIA

中國香港網絡安全協會
HONG KONG CHINA NETWORK SECURITY ASSOCIATION

Optimists for change

Sia is a next-generation, global management consulting group—born digital, augmented by data, enhanced by creativity, and driven by responsibility. We partner with clients to resolve challenges and capitalize on opportunities. We believe that in today's world of change and disruption, optimism is a force multiplier.