FROST & SULLIVAN

CENTER FOR CYBER SAFETY AND EDUCATION

(ISC)²

Booz | Allen | Hamilton

strategy and technology consultants

Alta ASSOCIATES EXECUTIVE SEARCH

2017 Global Information Security Workforce Study

Benchmarking Workforce Capacity and Response to Cyber Risk

A Frost & Sullivan Executive Briefing

INTRODUCTION

Cybersecurity professionals worldwide face an ever-evolving threat landscape that many feel they are ill-equipped to manage. Data breaches at corporations, educational institutions and government agencies continue to erode public confidence in the state of cybersecurity. The emergence of consumer goods such as wearable devices and self-driving cars, alongside the increasing connectivity of the systems managing critical infrastructure such as power plants and traffic signals are creating new threats to public safety, privacy, and economic stability.

The Center for Cyber Safety and Education partnered with (ISC)^2, Booz Allen Hamilton (Presenting sponsor), Alta Associates (Gold sponsor), and Frost & Sullivan to examine the state of the response to these developing risks in the 2017 Global Information Security Workforce Study (GISWS). This, the 8th edition of the Study, which has been running since 2004, reveals insights from an unprecedented number of respondents; 19,641 cybersecurity professionals representing 170 countries.

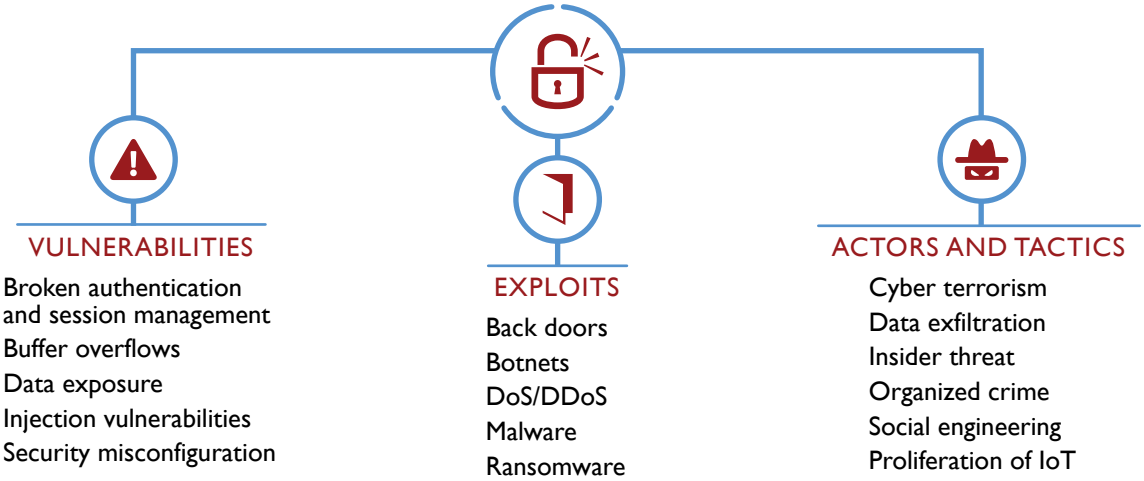
This executive summary of the findings highlights their top concerns. Two thirds indicated that there are not enough cybersecurity workers in their organizations to meet the challenges they currently face. This year's Study reveals we are on pace to reach a cybersecurity workforce gap of 1.8 million by 2022, a 20% increase over the forecast made in the 2015. It also reveals trends and insights into how hiring managers are responding and what organizations can do to attract, enable and retain the cybersecurity talent necessary to combat the risks in today's ever evolving threat environment.

THREATS AND THREAT ACTORS

Threats have evolved rapidly in recent years, and are no longer the domain of a limited number of skilled individuals. The malware-for-hire phenomenon has substantially lowered the bar for cybercriminals as lacking the technical know-how is no longer a barrier for those that can rent a bot net, exploit kit, or ransomware package.

Overall cybersecurity professionals have to contend with an increasing velocity of malware hitting their networks at a relentless pace. The GISWS tracks the level of concern with which security professionals regard particular threats. In 2017, threats of most concern were as follows:

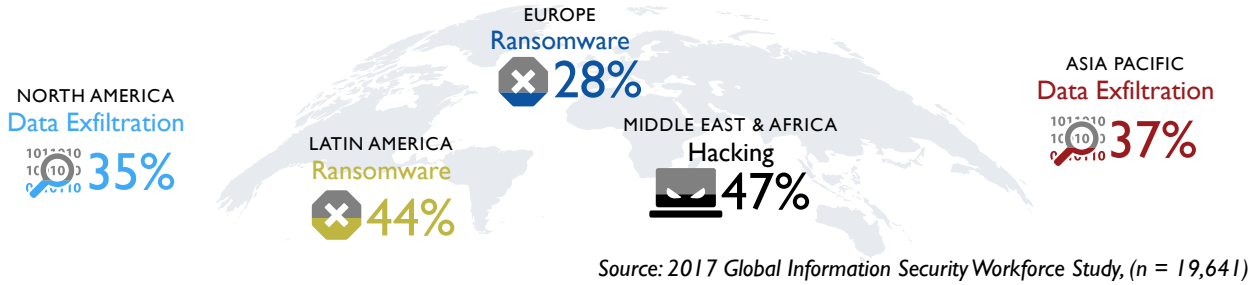
Exhibit 1: Threats of Most Concern



Source: 2017 Global Information Security Workforce Study

Globally, data exposure is the top concern for information security professionals, regardless of their geographic location. There are, however, some regional discrepancies when considering other top-of-mind threats. Data exfiltration is a top worry in North America and APAC, however, in LATAM and Europe, ransomware is top of mind. In the Middle East & Africa, the broad act of hacking is identified as a primary concern, possibly suggesting professionals here are being affected by a broad set of motivations and outcomes.

Exhibit 2: Top Concerns Globally



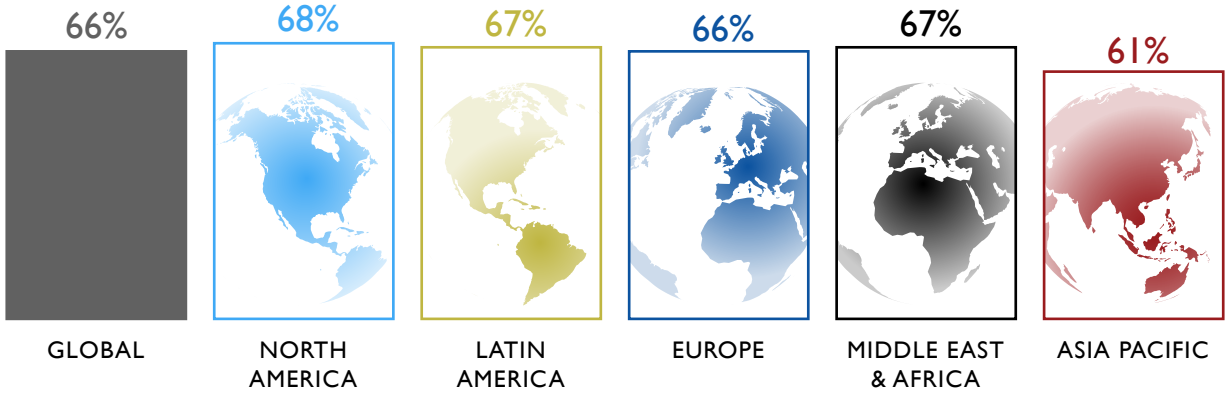
Source: 2017 Global Information Security Workforce Study, (n = 19,641)

The data clearly demonstrates much work is yet to be done to secure businesses, government agencies and organizations of all sizes, and the critical importance of having a properly staffed, agile and reactive workforce. However, in the 2015 edition of the GISWS, 62% of information security workers reported having too few workers to address the threats they encountered. In 2017, that number has ticked higher, with 66% indicating that they do not have the staff necessary to address the threats, indicating that the shortage of information security workers is widening, as more sectors recognize the importance of deploying a skilled cyber workforce to protect their data.

UNDERSTANDING THE SKILLS GAP

In 2015, Frost & Sullivan forecasted a 1.5 million worker shortage by 2020. In light of recent events and shifting industry dynamics, that forecast has been revised to a 1.8 million worker shortage by 2022. This is reflected by the extraordinarily high number of professionals across the globe who indicate that there are not enough workers in their departments.

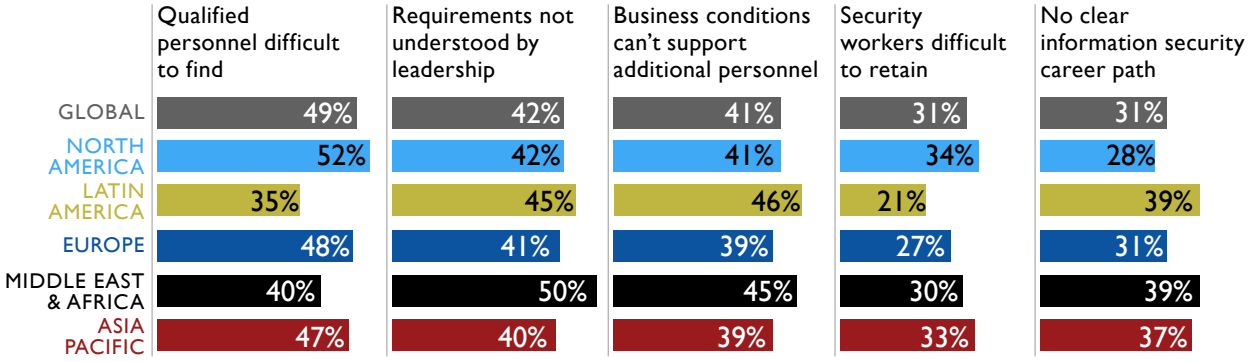
Exhibit 3: Too Few Information Security Workers in My Department



Source: 2017 Global Information Security Workforce Study, (n = 19,175)

Workers cite a variety of reasons why there are too few information security workers, and these reasons vary regionally, however, globally the most common reason for the worker shortage is a lack of qualified personnel. Nowhere is this trend more common than in North America, where 68% of professionals believe there are too few cybersecurity workers in their department, and a majority believes that it is a result of a lack of qualified personnel.

Exhibit 4: Reasons for Worker Shortage by Region

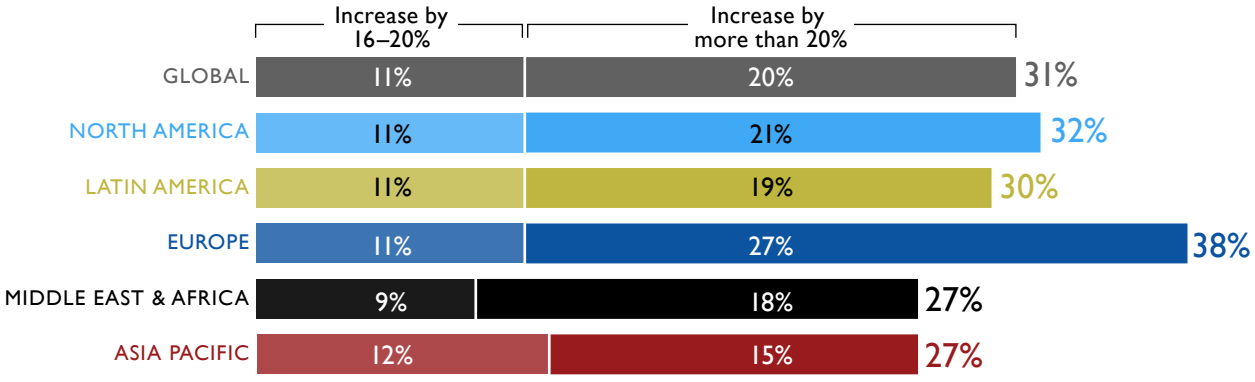


Source: 2017 Global Information Security Workforce Study, (n = 12,709)

Hiring is on the Rise

There is good news in an industry that urgently needs to address its worker shortage: globally a third of hiring managers are planning to increase the size of their departments by 15% or more. A great deal of hiring will be concentrated in Europe, where 27% of hiring mangers intend to expand their department by 20% or more, and a total of 38% will grow their department by at least 15%. The Middle East, Africa, and APAC can expect lower rates of hiring, however one in four hiring managers in each region still expect to see their departments grow by 15% or more.

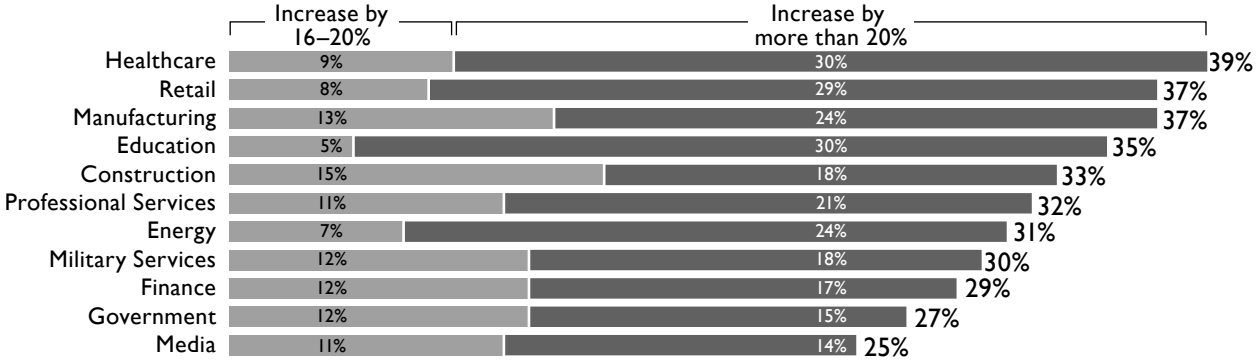
Exhibit 5: Hiring Managers Expecting to Increase Workforce by 15% or More By Region (Among Managers Expecting to Increase Workforce)



Source: 2017 Global Information Security Workforce Study, (n = 2,906)

Overall, 70% of hiring managers will increase their workforce this year: 30% wish to expand by 20% or more. Hiring managers looking to increase their workforces in the fields of healthcare, retail and manufacturing are particularly interested in expansion, with nearly 40% in each sector wishing to increase their workforce by 15% or more.

Exhibit 6: Hiring Managers Expecting to Increase Workforce by 15% or More By Industry (Among Managers Expecting to Increase Workforce)



Source: 2017 Global Information Security Workforce Study, (n = 2,906)

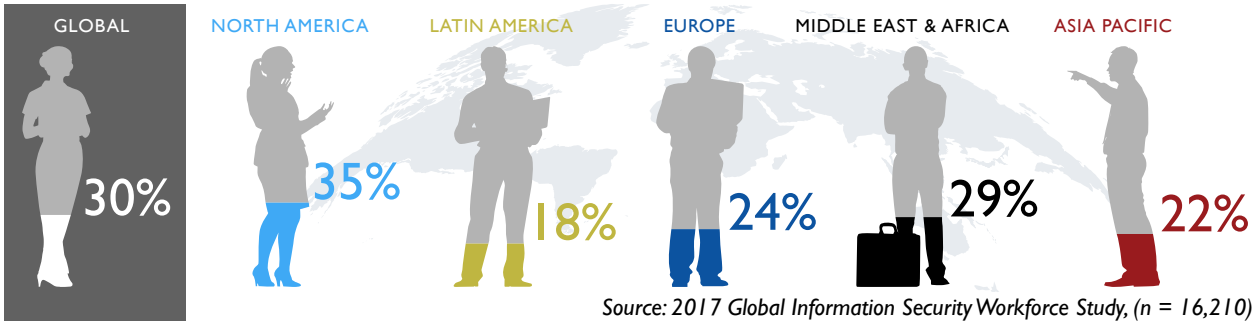
Globally, the most sought after positions are Operations & Security Management, with 62% of the workforce indicating that there are too few who occupy this position, followed by Incident & Threat Management and Forensics, at 58% globally. In fact, the latter position is in greater demand in LATAM (63%) and the Middle East & Africa (65%) than any other position.

Despite efforts by managers to increase hiring, historically demand has outpaced supply, and Frost & Sullivan projects that the gap will grow if current trends continue. Nearly 90% of the global workforce is male, a number that remains unchanged, and the majority arrive in information security with a computer science or engineering background. It is clear, as evidenced by the growing number of professionals who feel that there are too few workers in their field, that traditional recruitment channels are not meeting the demand for cybersecurity workers around the world. Hiring managers must therefore begin to explore new recruitment channels and find unconventional strategies and techniques to fill the worker gap.

EMBRACING A CHANGING WORKFORCE

It is not uncommon for cybersecurity workers to arrive at their jobs via unconventional paths. The vast majority, 87% globally, did not start in cybersecurity, but rather in another career. While many moved to cybersecurity from a related field such as IT, many professionals worldwide arrived from a non-IT background.

Exhibit 7: Percentage Who Came from Non-IT/Engineering Background (Among Those Who Did Not Start in CyberSecurity)



Source: 2017 Global Information Security Workforce Study, (n = 16,210)

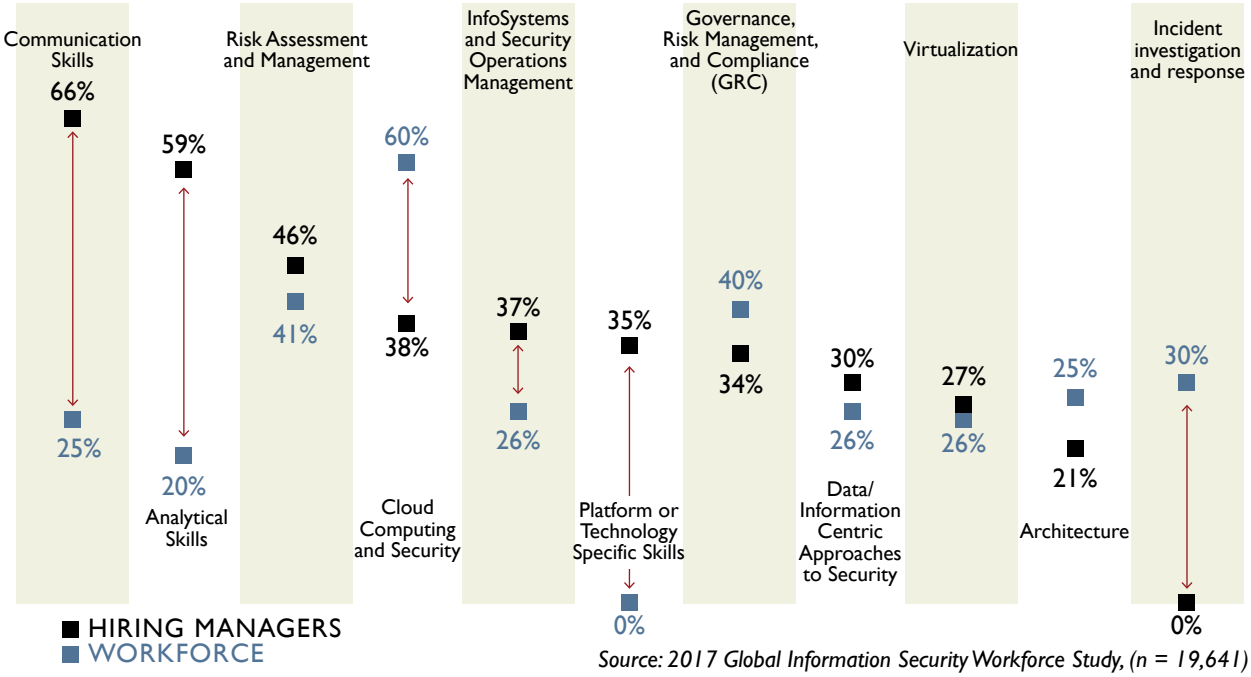
Previous non-technical careers are diverse, including business, marketing, finance, accounting, or military and defense. Individuals with non-technical previous careers often rise to become key decision makers in their organizations: globally, 33% of executives and C-Suite professionals began in a previous non-technical career. This illustrates the value of, expanding horizons beyond traditional technical recruitment channels. It will be important, if not essential, to consider the relevant educational foundations, training and professional

development opportunities that support the breadth of people with potential to enter the field in order to fill the worker shortage.

The New Recruit vs. Hiring Manager Disconnect

In addition to looking for non-traditional hires, hiring managers must be aware that their expectations for new hires do not correspond with workers' priorities for a successful career. The top skills that are prioritized by hiring managers are communication skills and analytical skills, while workers prioritize a slew of technical skills above communication and analytical skills. This suggests not only a disconnect between hiring managers and worker expectations, but a breakdown in communication of the desired traits and skills that managers are looking for in new hires.

Exhibit 8: Top Skills, Workforce (for Career Success) Versus Hiring Managers (for Hiring Workers)



Source: 2017 Global Information Security Workforce Study, (n = 19,641)

Hiring Managers Face External Pressures

Unemployment among information security professionals sits at only 2% globally. Low unemployment combined with a significant worker shortage inflates wages at a rate that dramatically outpaces economic growth; in North America, an information security worker is paid, on average, $120,000 per annum. Forty percent of North American workers under the age of 35 earn $100,000 or more. It is therefore not surprising that in the GISWS Meet the Millennials[1] study, compensation was a not a primary concern for Millennials globally. That same study found that Millennials were leaving their jobs at unprecedented rates: 28% had changed their job voluntarily in the past year. This revolving door of employment is not limited to young workers; globally, 21% of information security workers had changed jobs voluntarily in the past year.

The combination of virtually non-existent unemployment, a shortage of workers, the expectation of high salaries, and employees who leave companies at rates that only increases among younger generations creates

1 https://iamcybersafe.org/research_millennials/

both a disincentive to invest in training and development and a conundrum for prospective employers: how to hire and retain talent in such an environment?

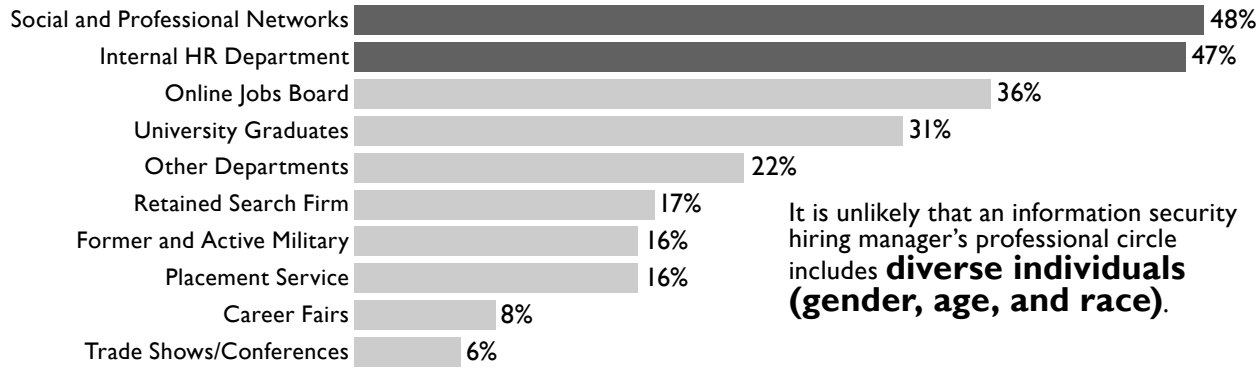
The solution lies in meeting the changing workforce with new hiring and recruitment, and professional development strategies, beginning with improved communication of expectations and, importantly, expanding reach beyond traditional channels.

ADAPTING RECRUITMENT STRATEGIES

As has been previously mentioned, the information security workforce is overwhelmingly dominated by men, and The GISWS Women in Cybersecurity[2] describes in detail many of the barriers, including different forms of discrimination, faced by women in the field. In addition, young workers are more likely to express lower levels of satisfaction than their older peers, and are the most likely to leave their job in favor of another. Addressing the underrepresentation of women in cybersecurity and increasing loyalty among young people are two important ways companies can begin to fill the 1.8 million worker gap projected for 2022.

This report has demonstrated that not only do nearly a third of the existing workforce come from a non-technical background, many of them had great success and have risen to the rank of executive or C-Suite. Hiring managers and recruiters must acknowledge their contribution. In order to fill the worker shortage, current methods of hiring and recruiting must be adapted to keep pace with the changing workforce, and this includes exploring non-traditional channels of recruitment. Seventy percent of hiring managers believe there are too few workers in their department, and 31% intend to substantially increase the number of employees in their departments. That said, the top recruitment tool favored by cybersecurity hiring manages remains their social and professional networks, followed closely by their organization's HR department.

Exhibit 9: Preferred Recruitment Sources Among Hiring Managers



Source: 2017 Global Information Security Workforce Study, (n = 4,767)

It is highly unlikely that a manager's professional circle includes many individuals from diverse backgrounds, or many women and young people with the potential to move into the profession. Clearly, new recruitment practices are needed, particularly ones that move away from prioritizing existing experience in the field. When considering a new applicant for a position, 94% of hiring managers indicate that existing experience in the field is an important consideration.

Current practice creates barriers to entry that both limits the breadth of expertise attracted to the profession, and the ability to address the skills gap itself.

2 https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

SECURITY READINESS AND JOB SATISFACTION

Envisioning the Needs for Asia-Pacific Information Security Professionals

Survey of 3,309 cyber and information security professionals in the Asia-Pacific region.*

* Asia-Pacific region includes China, Hong Kong SAR, India, Japan, Malaysia, South Korea, Singapore, Australia, New Zealand and rest of Asia

TECHNOLOGY MATURITY IN COUNTRIES IMPACTS PERFORMANCE TOWARD ATTACKS

PERFORMANCE IN A CRISIS

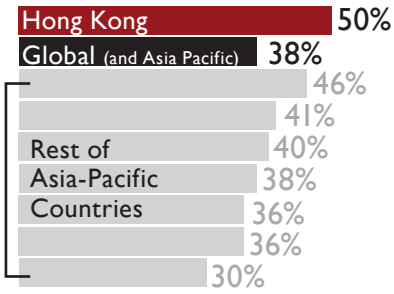
Having Systems in Place to Prepare for an Incident

India 71% — Perform Worse than last year

Japan 60% — Perform the Same or Better than last year

RESOURCES ARE STRETCHED IN ATTACK RECOVERY

RECOVER FROM ATTACK IN A WEEK



In Hong Kong,

72%

of security professionals work more than

41 hours per week

SECURITY SKILLS IN DEMAND

Asia-Pacific

58%

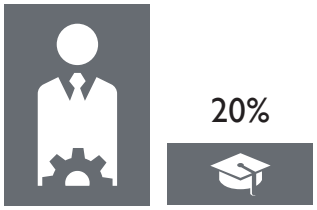
Operations and Security Management

56%

Forensics, Incident, and Threat Management

HIRING TREND

IMPORTANCE DURING HIRING



Relevant Experience

Relevant Degree

31%

of Millenials rely on their internal HR department to recruit talent, less than the rest of the age groups at 40%

EDUCATION AND TRAINING INCREASE JOB SATISFACTION

INCREASED EDUCATION AND TRAINING

46%

Asia-Pacific

57%

India

Correlates to **HIGH** Job Satisfaction

JOB SATISFACTION VARIES

Very Satisfied

Asia-Pacific 22%

29% India

29% Australia

Dissatisfied

17% China

IMPROVE SECURITY SYSTEMS AND TRAIN OFTEN

Empower information security professionals with the best security systems and increase training for the skills in demand

CENTER FOR CYBER SAFETY AND EDUCATION · (ISC)² · Booz | Allen | Hamilton strategy and technology consultants · Alta Associates · FROST & SULLIVAN