BUILDING A BIGGER PIPELINE

THE 2015 (ISC)² GLOBAL WORKFORCE STUDY SHOWS WE MUST FUNNEL MORE PEOPLE INTO INFORMATION SECURITY…AND SOON

BY **ANNE SAITA**

ANGELA MESSER WAS excited when she read the results of the 7th (ISC)²® Global Information Security Workforce Study (GISWS), not by the growing shortage of qualified security professionals but by the call to action the findings portend.

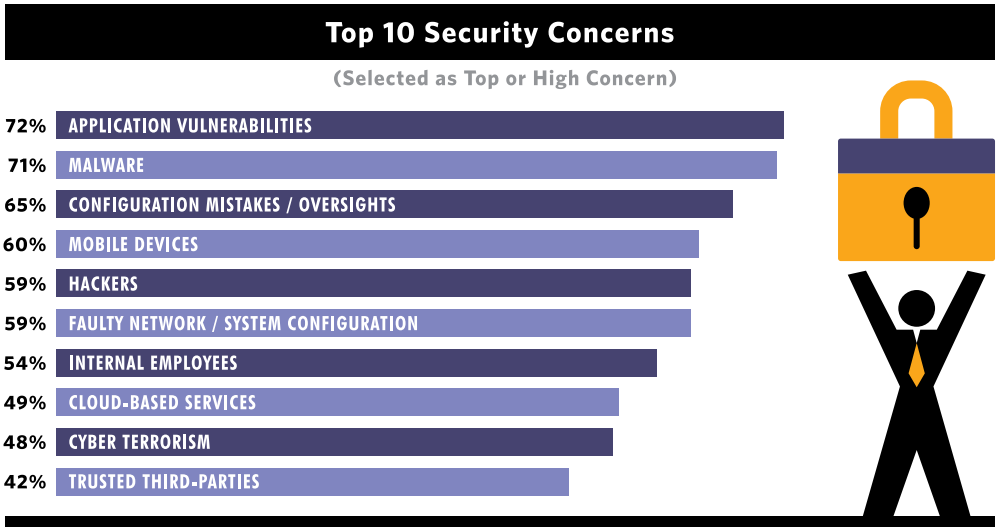
"We all say we need more talent, but what we're now finally focusing on is what to do to bend the demand," she says.

"In the last several years, cyber has hinged on awareness, not just from the IT security staff but the CISO and CIO," continues Messer, an executive vice president who leads the predictive intelligence business at Booz Allen Hamilton, an (ISC)² partner in the study. "The C-suite now gets it, so there is now more acknowledgement of just how important these skills are. This is a big step in showing we're well on that path."

A big step, perhaps, but what it may need are huge leaps.

This year's GISWS is based on nearly 14,000 respondents globally, comprised of both (ISC)² members and non-members. The majority of respondents are located in North America (with a decent turnout from pros in Asia and Europe). A third of them hold management or executive positions, and two-thirds work at companies with 10,000 employees or more.

This year's GISWS is based on nearly 14,000 respondents globally.



INFOGRAPHICS BY ROBERT PIZZO

RETURN TO CONTENTS

The most significant finding from the study is the growing gap in skilled labor at a time when transformative technologies like cloud services, software-defined data centers and the proliferation of mobile end points are taking over enterprises.

The workforce shortage has allowed those already in the field to command higher salaries, especially if they carry security-specific credentials, but those bigger paychecks come at a cost: higher demands on the workers. That may be why, despite the vast majority of respondents saying they like their current jobs, almost 20 percent sought new positions last year.

"Right now, there are 200,000 open infosec positions in this country that we can't fill."

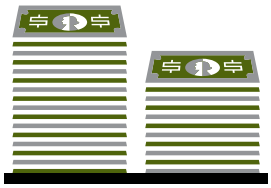
—JOAN PEPIN, CISO, Sumo Logic

"Right now, there are 200,000 open infosec positions in this country that we can't fill," says Sumo Logic CISO Joan Pepin shortly after results were released in April.

That fulfillment problem may be due to too few companies offering entry-level positions and too many wanting only ideal candidates.

"The attitudes of these hiring managers absolutely need to change," says Mark Aiello, president of Cyber 360, an HR placement firm focused 100 percent on cyber security and a study partner. "We keep hearing that there's a shortage of candidates, and I say, 'No. What there is is a shortage of perceived perfect candidates. There is not a shortage of candidates.'"

If those attitudes fail to change and emerging technologies continue their rapid adoption, the survey predicts that this workforce shortage could widen by 2019 to 1.5 million available positions.



(ISC)² members earn 35% more on average than their non-member counterparts—$103,117 vs. $76,363.

STUCK IN NEUTRAL

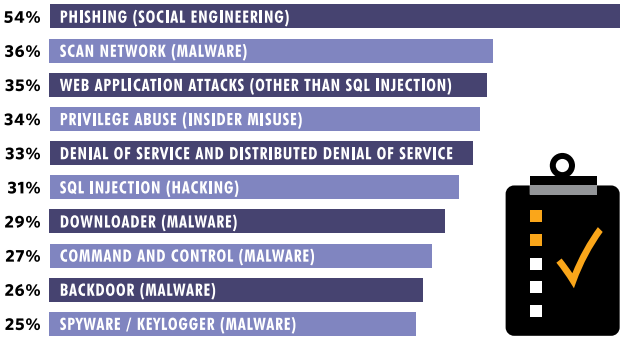
"We are spending more money, but we are not getting any better at it—that's what our survey respondents are saying," Frank Dickson, research director for information and network security at Frost & Sullivan, told an audience at April's RSA Conference in San Francisco.

Part of that spending increase appears to bigger salaries for those holding (ISC)² certifications. Worldwide, the average annual salary was US$97,778. Within that figure, however, (ISC)² members earn 35 percent more on average than their non-member counterparts—$103,117 vs. $76,363.

"I always say security certifications do matter, because you can make more money if you have one," Mark Aiello, president of the recruiting firm Cyber 360, says. "This study validates that."

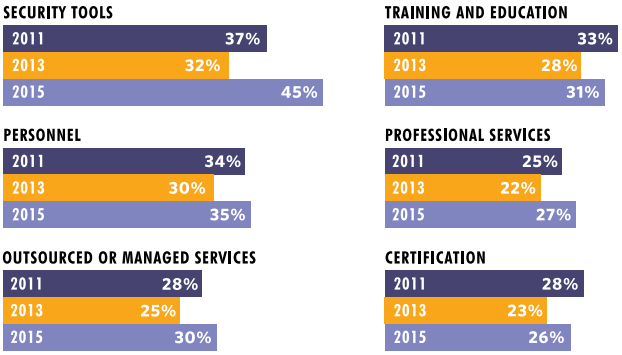
Top 10 Common Threat Techniques

(Selected as Top Two on a Five-Point, Not-Common-to-Very-Common Scale)



Where Increases in Information Security Are Projected

(Percent of Survey Respondents)



The study also revealed how companies are coping in the short-term with the gap in skilled labor: by essentially pushing security-related functions on other staff who have little to no information security experience. This "force multiplier" can cause slowdowns and other suboptimal results that cyber criminals are all too eager to exploit.

Part of the problem is that information security is a specialized field, requiring years of experience and high critical thinking skills. This is creating a shift in higher education, where curricula are being reconfigured based on current needs, and more scholarships are emerging to encourage students, particularly women and minorities, to consider information security as a college degree.

"Something I hear over and over again is that we DO have students graduating from schools, but there are no entry-level positions for them."

—ELISE YACOBELLIS, director of development, Americas Region, (ISC)²

But the profession also requires practical experience, and companies have been slow to provide those opportunities.

"Something I hear over and over again is that we do have students graduating from schools, but there are no entry-level positions for them. I'd challenge organizations to build internships and entry-level positions so more people gain experience," Elise Yacobellis, director of development, Americas Region for (ISC)², said during the RSA panel.

"If you do not put a stake in the ground now, we're never going to see that growth," she added.

'IT TAKES A VILLAGE' TO RAISE A CYBER WARRIOR

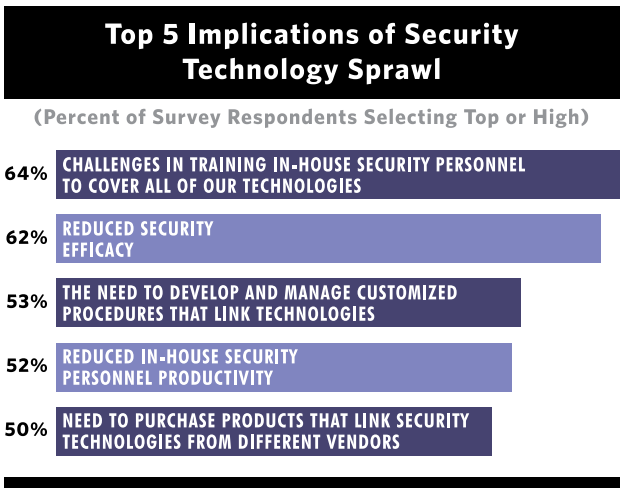
With television programs like *CSI Cyber* and *Scorpion* and action movies like *Blackhat*, Hollywood has helped update the image of cybersecurity workers from cellar-dwelling dweebs to the cool kids, but if we're going to truly fill that pipeline with future cyber security warriors, we need to reach out to kids in childhood.

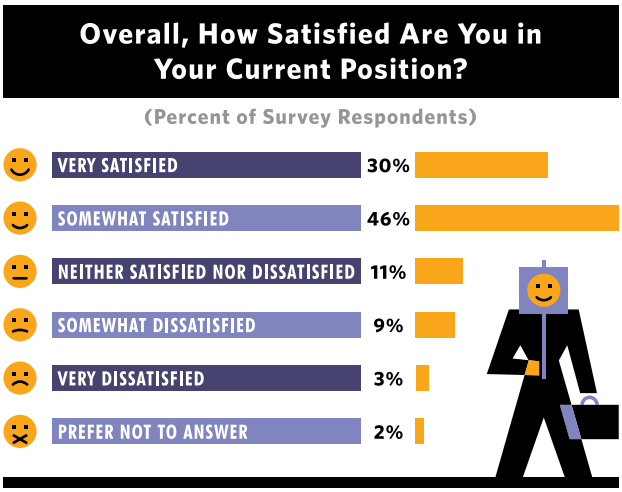
"It takes a village to solve the supply problem," says Booz Allen Hamilton's Messer.

Experts like Messer believe recruitment should start no later than middle school, when students' attitudes and aptitudes in science, technology, engineering and math begin to take shape. Games and hackathons can help locate raw talent, and scholarships can help fund both college and non-traditional career paths—such as cybersecurity grants for veterans in transition.

"I think our government needs to help with people's education so that they can go to school without taking on a lot of debt," Pepin says. "And we need to do something about the horrible technology gender gap, which has women leaving at a record rate."

((ISC)² will release survey findings on women in information security this fall).





A Salary Comparison

WORLDWIDE	(ISC)² MEMBERS			NON-MEMBERS		
AVERAGE ANNUAL SALARY	$98,605	$101,015	$103,117	$78,494	$75,682	$76,363
SURVEY-OVER-SURVEY		2.4%	2.1%		-3.6%	0.9%
MEMBERSHIP PREMIUM	26%	33%	35%			
	2011	2013	2015	2011	2013	2015

Certification *Does* Pay Off

US-BASED SECURITY ANALYSTS IN PRIVATE SECTOR	(ISC)² MEMBERS WITH CISSP CERTIFICATION			NON-MEMBERS WITHOUT CISSP CERTIFICATION		
AVERAGE ANNUAL SALARY	$93,027	$94,316	$99,759	$76,402	$76,957	$81,301
SURVEY-OVER-SURVEY		1.4%	5.8%		0.7%	5.6%
MEMBERSHIP PREMIUM	22%	23%	23%			
	2011	2013	2015	2011	2013	2015

Higher education also needs to offer courses that meet the dynamic skills required for our current and future workforce.

Higher education also needs to offer courses that meet the dynamic skills required for our current and future workforce. Programs such as (ISC)2's Global Academic Program help bridge the knowledge gap through a joint framework with a growing network of colleges offering degrees in information security.

"We need to think outside the box to solve this problem," Messer says. For instance, Booz Allen Hamilton has a Cyber SIM program within its internal "Cyber University" that takes a challenge-based approach to threat response. The training platform has proven so popular that the company's clientele now want similar simulations to recruit, retain and retrain their own security staffs.

Cyber SIM, GAP and other initiatives are a start. But, as Frost & Sullivan's Dickson and Michael Ruby, VP of Research, write in a white paper, we have a long way to go and not a lot of time to get there:

"As a concerned and collaborative effort across organizations and disciplines, a security workforce that can address the evolving needs and complexities of cybersecurity and usher in safe and security cyber innovation is possible.

"This possibility; however, cannot wait. The time to act is clearly now." ●

ANNE SAITA *is editor-in-chief of* InfoSecurity Professional.

How Would You Rate the Importance of Each of the Following in Contributing to Being a Successful Information Security Professional?

(Percent of Survey Respondents Selecting Top Two Points on a Five-Point Importance Scale)