Study |

IT Professionals are a Critically Underutilized Resource for Cybersecurity

(ISC)²

INSPIRING A SAFE AND SECURE CYBER WORLD

MISSED OPPORTUNITY

According to (ISC)² research, most organizations do not have enough skilled cybersecurity professionals on staff, and their readiness to discover and recover from cyberattacks has declined over the past year. Despite those findings, enterprises and government agencies fail to give IT professionals – the very individuals implementing and operationalizing security strategies for most organizations – the training and responsibility they need to take on a more proactive cybersecurity role. Moreover, many IT professionals feel their security guidance is ignored by leadership.

THE UNTAPPED CYBERSECURITY RESOURCE

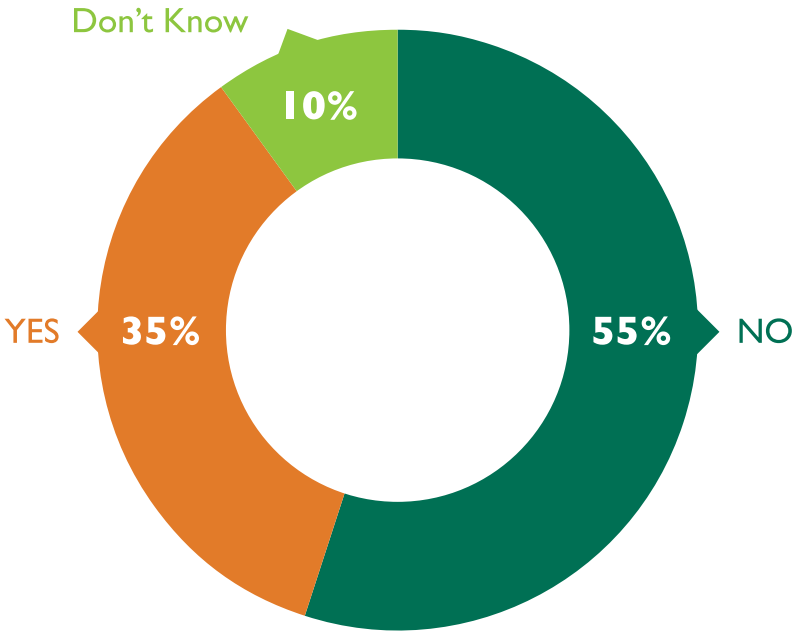
(ISC)² research based on responses from more than 3,300 IT professionals who participated in the 2017 Global Information Security Workforce Study finds IT professionals are an underutilized and potentially untapped resource for many organizations struggling with their cybersecurity workload.

Close to half (43%) of IT pros said their organizations don't provide adequate resources for IT security training and professional development, and that their ability to defend against cyberattacks has declined in the past year.

As the people on the frontlines implementing and operationalizing cybersecurity strategies every day, IT teams are working hard to prevent cyberattacks and lead remediation efforts when they occur. But despite their contributions, their opinions about how to protect their organizations are often ignored. Only 35% agreed their security suggestions are followed, while 28% said they are asked for advice, but it falls on deaf ears.

Security Certifications Not a Priority

Only 35% of respondents said their organization requires IT staff to have a cybersecurity certification



Nearly two-third of respondents (63%) said their organizations have too few cybersecurity workers, and more than half (55%) said their employers don't even require IT staff to hold security certifications.

Compounding the problem, just over half (51%) said their systems are less able than a year ago to handle a cyberattack. Only 11% said their organization can discover a breach immediately.

Nearly half of participants attribute the brunt of these issues to a leadership problem, with (49%) saying leadership in their organizations lacks enough understanding of cybersecurity requirements.

TEPID COMMITMENT

Data suggests leadership's attitude toward cybersecurity, both in the areas of technology and human resources, is problematic. It appears to manifest itself in what could be considered an - at best - moderate commitment to raising IT staff's security expertise levels through training and certification.

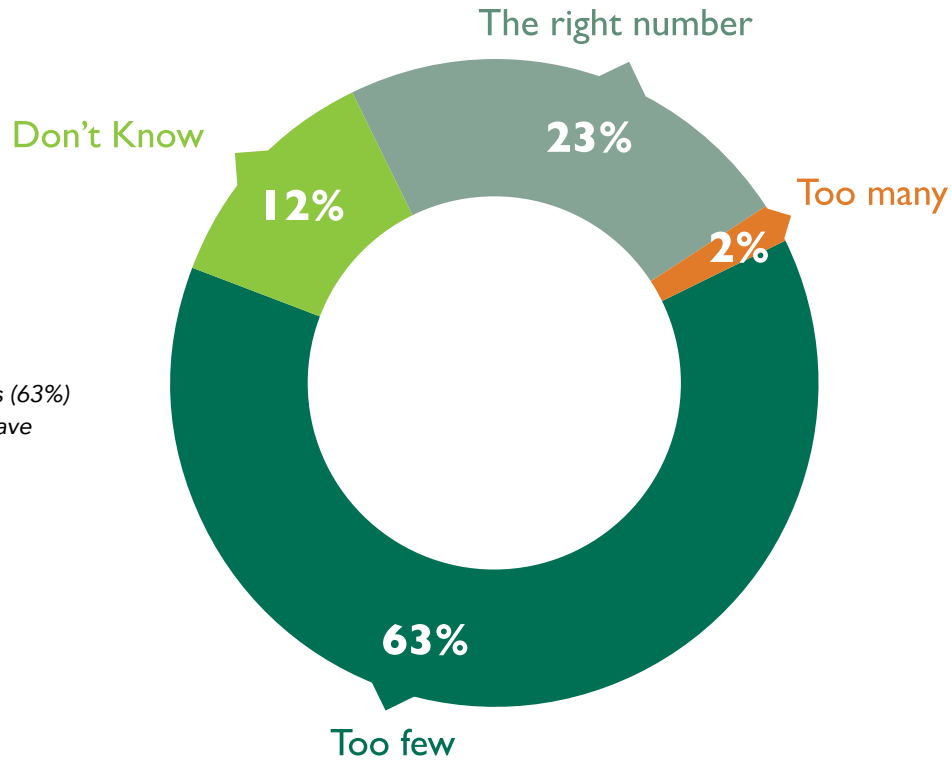
It is possible employers are more focused on hiring people who already bring in the required qualifications and expertise, as opposed to training existing team members. This would reflect a common pattern in other areas of IT, where employers often are frustrated by not finding talent with the requisite expertise or experience.

Asked about hiring priorities, survey participants placed great emphasis on recruiting candidates with relevant security experience (93%). Two-thirds of respondents termed relevant experience "very important," while 26% called it "somewhat important." Knowledge of cybersecurity concepts was deemed very important by 65% of respondents and somewhat important by 27%.

There was less emphasis on knowledge of relevant regulations, with a combined 74% of respondents calling it very or somewhat important. IT certifications fared slightly better, with a combined 75% rating, while IT security or related college degrees didn't get the nod from half of respondents (48%).

Help Needed

Nearly two-thirds of respondents (63%) said their organization doesn't have enough cybersecurity workers.

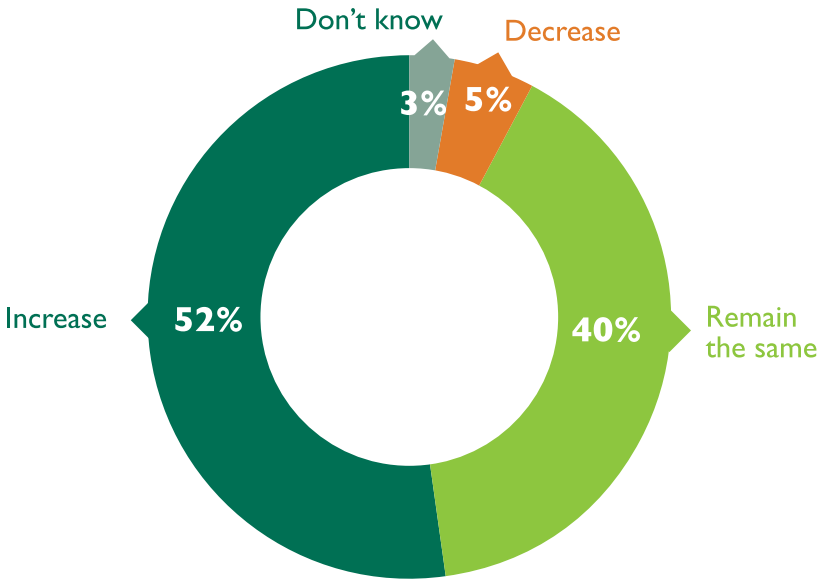


UNREALISTIC EXPECTATIONS OR CONFUSION?

These findings suggest some unrealistic hiring expectations. They appear to explain why about a third (34%) of respondents said it's hard to find qualified candidates. Considering the evolving nature of the threat landscape, hiring people with all the requisite experience and knowledge is a challenging prospect. Even experienced security pros need constant refresh because the threat landscape changes rapidly with 400,000 new malware samples released daily.[1] Security knowledge can get stale without continuing education.

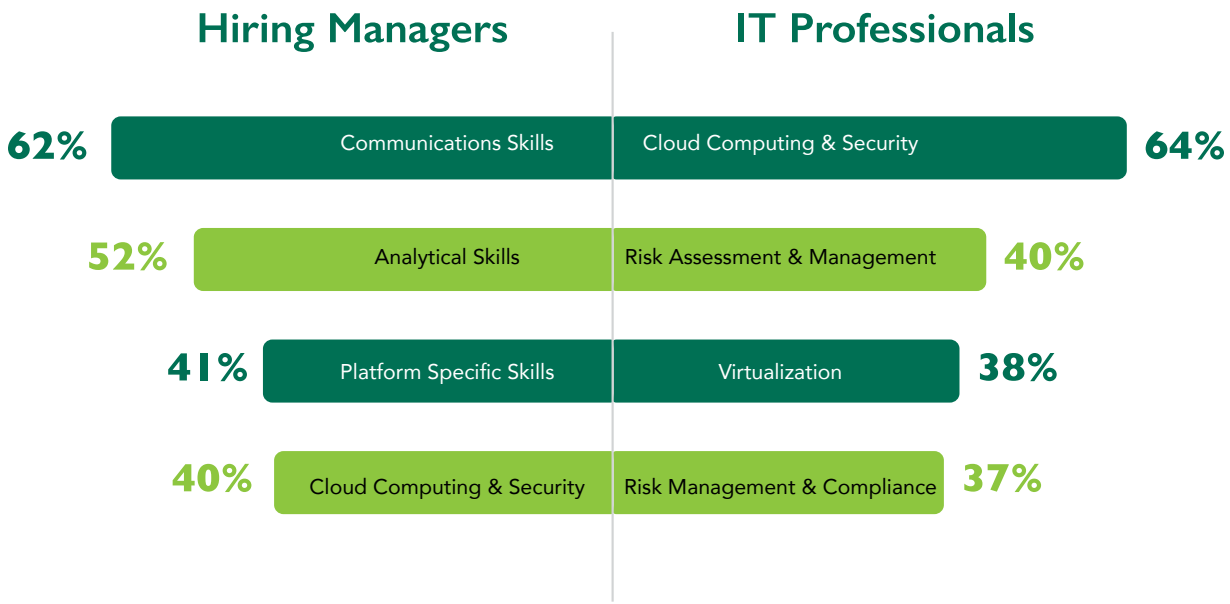
Not Enough Cybersecurity Training

Only 52% of IT professionals expect the security training and education they receive to increase over the next year.



Skills Disconnect

Communications and analytical skills ranked as the top two skills and competencies hiring managers look for, but cloud security and risk assessment are what front-line professionals say their organizations need.



Another possible explanation for the hiring expectations is IT hiring managers know that since their employers aren't likely to provide adequate on-the-job training, they might as well get as much expertise in new hires as possible.

Perhaps another explanation has its roots in relatively new organizational changes in many enterprises. In recent years following many high-profile data breaches, the role of Chief Information Security Officer (CISO) has risen to prominence in corporate boardrooms and even within government agencies. While CISOs have a critical role to play in developing and driving sound cybersecurity and risk management strategies, many tactical, day-to-day security functions remain within the purview of IT and the Chief Information Officer (CIO). This may create additional uncertainty about who is ultimately responsible for cybersecurity. This must be viewed and accepted as a shared responsibility, and IT teams need to be seen as an existing asset to help bolster an organization's defenses by adopting best security practices throughout all IT implementations.

Whatever the explanation, a long-term investment in cybersecurity training and education is lacking in IT, but certainly advisable if organizations want to properly protect themselves.

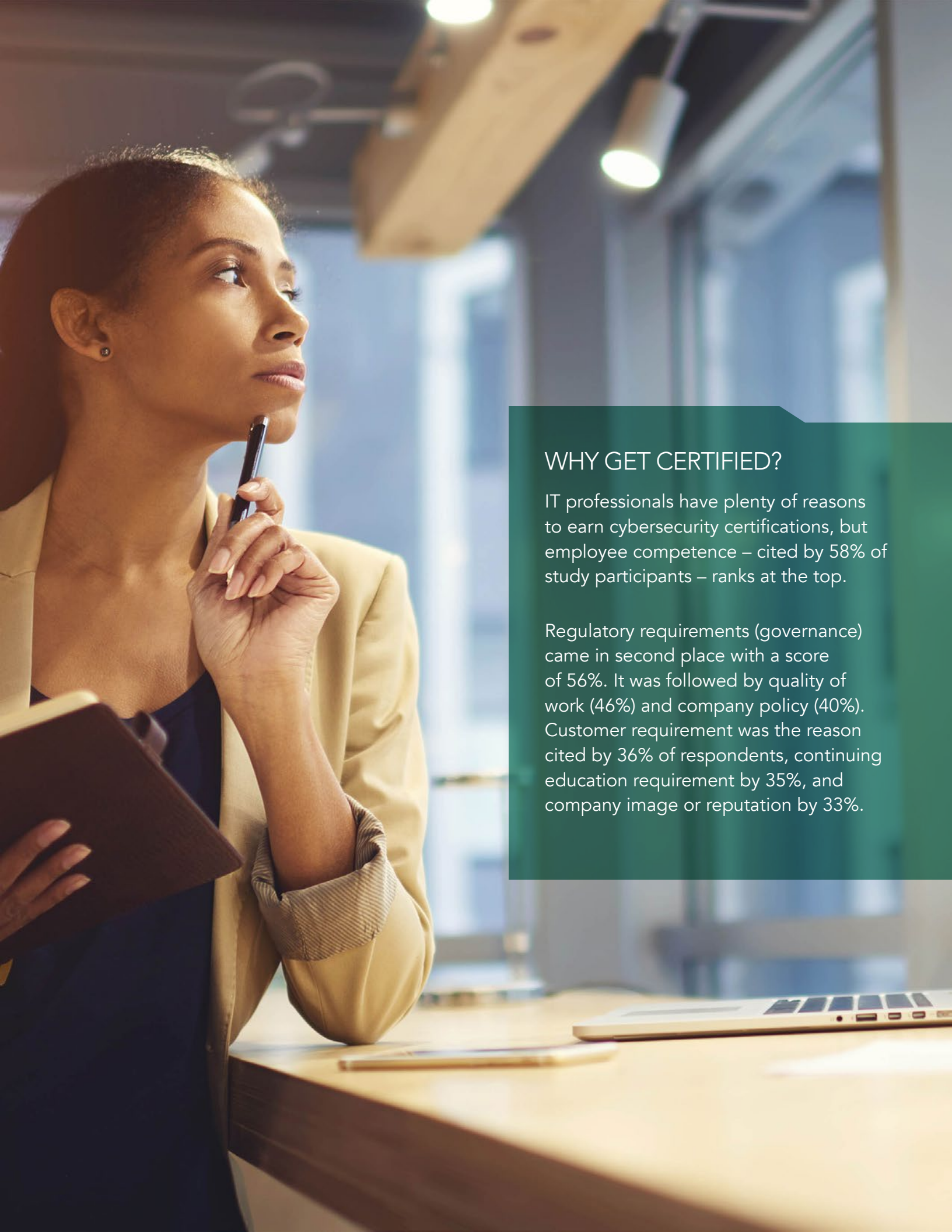
WHO PAYS?

Even though providing education can help set a career path for IT security pros, the study reveals that only one-third of respondents (34%) get training paid for by their employers, while 29% said employers share the cost. Another third (34%) said they have to pay for all of their own security education.

Training and certification for IT professionals in charge of security is important not just because the workers need updated, provable skills, but also because a well-trained, knowledgeable staff is more likely to keep a company safe from attack. Considering the potential costs of an attack to their brands and reputations, organizations may want to consider paying for training as an investment in the business.

In addition, it's likely that if organizations made a stronger commitment to training and certifications by contributing the cost, more IT pros would take advantage of them.

The study suggests that providing education can help with employee retention. One quarter of respondents (25%) said one of the reasons organizations don't have enough security staff is because they cannot retain them. Another reason, cited by 36% of respondents, is a lack of career path for IT security pros. Not surprisingly, budget also plays a role, with 44% of respondents saying "business conditions can't support additional personnel."



WHY GET CERTIFIED?

IT professionals have plenty of reasons to earn cybersecurity certifications, but employee competence – cited by 58% of study participants – ranks at the top.

Regulatory requirements (governance) came in second place with a score of 56%. It was followed by quality of work (46%) and company policy (40%). Customer requirement was the reason cited by 36% of respondents, continuing education requirement by 35%, and company image or reputation by 33%.

> “An investment in educating people is essential to a robust defense posture.”

STATUS QUO

The need for training isn't being completely ignored, considering that over the past 12 months, 44% of organizations increased security training. This trend, however, was moderated by 41% that kept it the same and 13% that actually decreased it. So the overall effect is to keep the status quo.

Looking into the next 12 months, 50% of respondents said they expect spending on training and education to remain the same, while 33% said it will increase. Not surprisingly, the numbers for certification plans were almost identical, with 51% saying they expect more of the same and 30% predicting an increase.

Based on these findings, the tendency going forward is to keep spending on training and certification at current levels. The area expected to see the greatest spending increase is in security tools (47%) – an understandable focus considering 51% of respondents said their systems are less ready to defend against an attack compared to a year ago. Even so, 40% of respondents said they expect spending on tools to remain level.

And while spending on technology to keep up with threats makes sense, it's important to recognize cybersecurity isn't strictly a technology play. An investment in educating people is essential to a robust defense posture.

WHAT TRAINING IS BEST

Computer-based capabilities may continue to displace human functions, but when it comes to security training, face-to-face settings are still hard to beat. That was one of the findings of the 2017 Global Information Security Workforce Study, in which 75% of respondents selected in-person training as their preferred method.

About half of respondents (49%) called live classroom training "very relevant," while 26% classified it as "somewhat relevant." In contrast, internet-based training got a 41% score in the "very relevant" column and 36% in "somewhat relevant," for a combined score of 77%. Overall, internet-based training edged out live classrooms by two percentage points, but fell short in the "very relevant" category.

VULNERABILITY LEVELS

When it comes to having robust defenses, the study shows IT workers tasked with security believe things could be better. Not only do nearly half of them (47%) believe their organizations are less ready to recover from a targeted attack, but 49% also believe they are less ready to discover an attack. Only 11% believe they can discover a breach immediately.

This is a serious concern because some advanced malware variants are designed to hide undetected in networks, quietly siphoning off data to hackers' command and control servers. By the time such a breach is discovered, plenty of intellectual property and private data may already have been stolen.

The survey found 29% of respondents believe they can recover from a targeted attack in one day, 37% in two to seven days and 18% said they don't know.

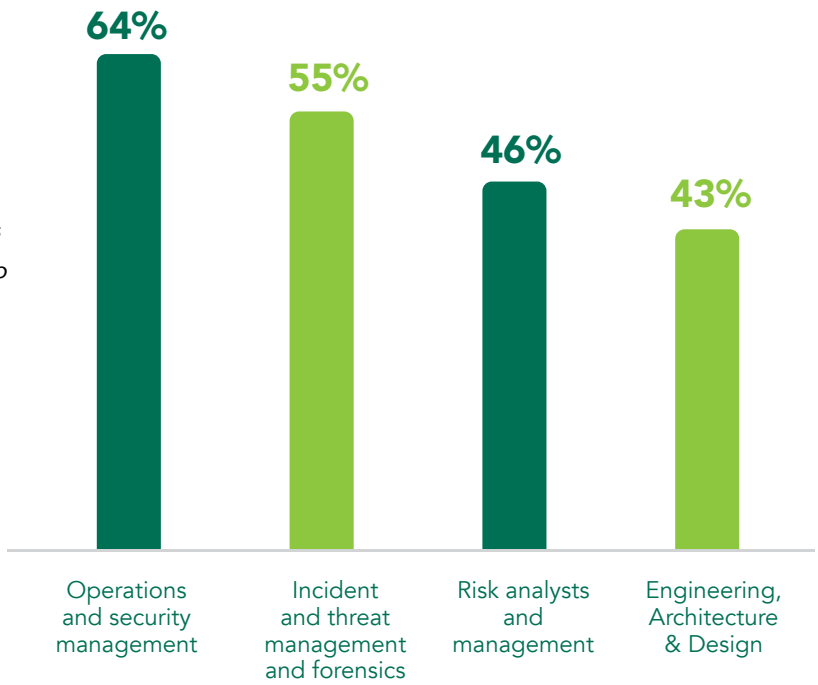
Potentially adding to organizations' security vulnerabilities is what respondents view as insufficient types of expertise in their organizations, including:

- Operations and security management – 64%
- Incident and threat management and forensics – 55%
- Risk analysts and management – 46%
- Engineering, Architecture & Design – 43%

To improve their security stance, organizations should be investing in these areas, especially considering how sophisticated and frequent cyber threats have become. For most organizations, filling these gaps would likely require a combination of new hires, training of existing staff to update their skills and investments in technology to address advanced threats.

Skills Deficit

IT professionals called out operations and security management as their top security need.



CONCLUSION

The 2017 Global Information Security Workforce Study reveals that leadership in the public and private sector needs to realize that IT staffers are dramatically underutilized when it comes to cybersecurity. Since IT professionals are usually the people tasked with day-to-day security operations, it behooves organizations to invest more in security training, education and certifications to strengthen their cyber defenses. Too many organizations are focused on the inability to find qualified cybersecurity professionals that they ignore a potential talent pool that is already on staff and familiar with their organization and infrastructure. The solution for many organizations lies in training and enabling IT professionals to take on broader security roles.

METHODOLOGY

The data in this report is based on the responses of more than 3,300 IT professionals who participated in the 2017 Global Information Security Workforce Study. One of the most in-depth studies of its kind, the Global Information Security Workforce Study surveyed more than 19,600 cybersecurity professionals to gain insight into a wide range of topics, including workforce trends and issues, professional development, demographics, salaries, top security concerns, job satisfaction and more. Sponsored by (ISC)², the Global Information Security Workforce Study was conducted by The Center for Cyber Safety and Education, a non-profit charitable trust committed to making the cyber world a safer place for everyone.

ABOUT (ISC)²

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, over 125,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Learn more at www.isc2.org.

[1] AV-Test, https://www.av-test.org/en/statistics/malware/

(ISC)²

INSPIRING A SAFE AND SECURE CYBER WORLD