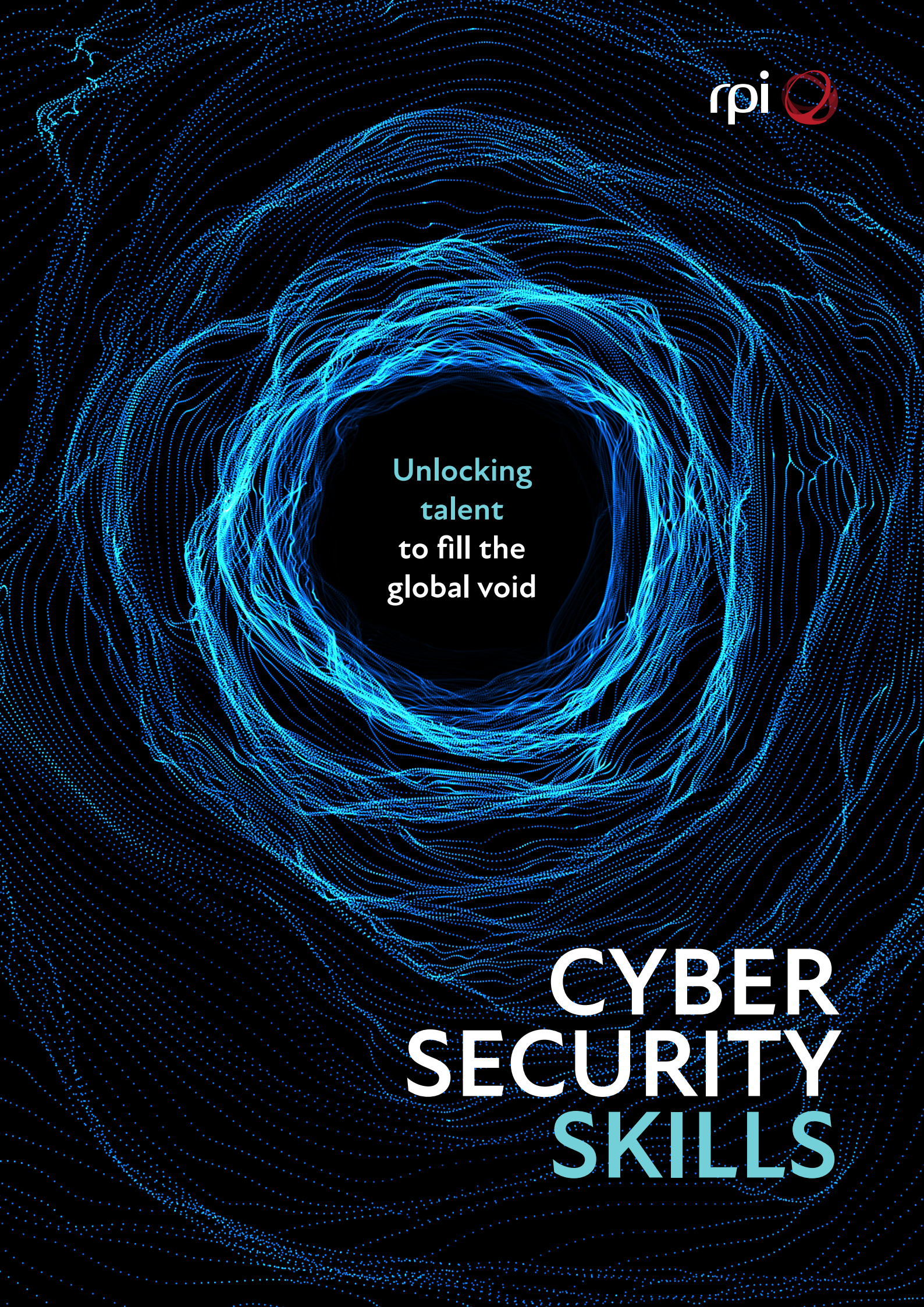

rpi
Unlocking
talent
to fill the
global void
CYBER
SECURITY
SKILLS

62%

of businesses report that their cyber security teams are understaffed

20%

say it takes over 6 months to find qualified candidates for cyber security positions

60%

report retention difficulties with their cyber security talent

Source: ISACA's 'State of Cyber security 2022'

If you're struggling to find the cyber security talent you need, you're not alone. The figures reveal a very stark talent gap, with organisations seriously struggling to attract and keep the professionals they need.

This is a guide to the current state of cyber security hiring: the roles, the state of regional employment markets, and the steps that businesses can take to secure the talent that they're missing.

The international view:
a regional snapshot of cyber skills shortages.

NORTH AMERICA

700,000
current US cyber security vacancies

561,000
in 2019

376,000
post pandemic

63% of North American business leaders say that cloud security is the most challenging role to fill.

EUROPE

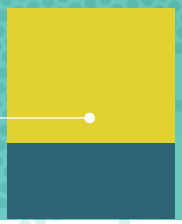
1 in 2 of european businesses identify a shortage of basic cyber security skills

Demand for cyber security skills has grown by 22% over the last year

MEA

100,000
estimated cyber skills shortfall

64% of Middle East firms are struggling to recruit and retain cyber security talent



LATIN AMERICA

441,000
cyber security talent shortfall in **BRASIL**

260,000
cyber security talent shortfall in **MEXICO**

APAC

Just 5% of IT professionals have sufficient technical knowledge and experience to analyse attacks on their network

42%
of data centre operators believe the region has enough cyber security professionals to fill its vacancies

Essential skills for cyber security professionals.

Cyber Security
It sounds obvious, but this includes not only the technical skill of cyber security, but also awareness of the innovations that cyber criminals are making, and a creative and proactive approach to anticipating threats and designing new barriers and safeguards.

Communication
Teams will frequently have to communicate with colleagues who aren't experts in IT or cyber security, and will need to explain concepts and technical issues accessibly.

Collaboration
Building new solutions and improving cyber security means listening to feedback, and consulting with colleagues.

Leadership
The more senior the cyber security hire, the more they will require management experience, and the ability to lead initiatives and secure buy-in from employees, sometimes company-wide.

Commercial awareness
An understanding of a business's goals, strengths, weaknesses, and ambitions will assist in understanding which are the most pressing threats and priorities from a cyber security point of view.

The roles that businesses need to fill.

Chief Information Security Officer
A CISO is ultimately responsible for protecting the company from cyber risk, guiding the security strategy, and educating the business on the risks. A CISO is especially important when a business is hoping to quickly scale its digital transformation, as rapid new developments mean extra vulnerabilities arise quickly.

Cyber Security Engineer
A Cyber Security Engineer designs and builds protective measures for a business's systems and data.

Cyber Security Analyst
A Cyber Security Analyst actively monitors the company's network, and proactively addresses weaknesses before an attack can happen.

Penetration Tester
In a way, the penetration tester is the opposite number to the cyber security analyst – they actively attempt to identify, exploit, and expose weaknesses in the business's cyber security, as if they were a malicious third party. That testing of course allows a company to reinforce areas that are shown to be vulnerable.

Attracting and retaining talent.

What can companies do to grow their cyber security workforce?

2.72m unfilled cyber security roles globally, and ISC2 calculates that the **global cyber security workforce needs to grow by 65%** for the world's organisations to adequately protect themselves from cyber threats.

Tap new wells of talent

The cyber security industry needs to embrace and retain talent from a broad range of backgrounds if it's going to overcome its talent gap – for instance, one glaring statistic about cyber security generally is that only a quarter of cyber security professionals are women.

While increasing diversity in the sector starts with making education accessible to a broad demographic, businesses will also play a crucial role by making sure they welcome a diverse range of talent from different backgrounds. It's fast becoming apparent that creating a more inclusive workplace will help businesses to access the cyber skills they need, particularly with increasing competition for those skills.

Better employer marketing

Does your marketing only target prospective customers, or do you run concerted campaigns to attract talent? You need talent to know you exist, and see you as one of the more appealing employers. In a candidate-driven market where competition for workers is so fierce, that takes real strategy, not just a few ads and a listing on job sites. You also need to make sure that your culture and values are being communicated effectively, as these are a real selling point to potential employees.

Plugging retention leaks

There are obvious things without which you might be a less competitive employer – more flexibility, better perks, better salaries might all lure talent away. Assuming you've assessed those, start looking deeper. Exit interviews or questionnaires might reveal patterns in why departing employees have chosen to leave, and they're useful, but in a sense they're also too late.

Don't be afraid to ask existing employees (anonymously) how they're feeling in terms of satisfaction, happiness, and burnout, what they would change about the company and their work if they could, and even what would persuade them to take a job elsewhere.