Deloitte.

JANUARY 2023

FINANCIAL SERVICES INDUSTRY
FEBRUARY 2023

Finding cybersecurity talent in an altered world

Contents

Since the onset of the pandemic, attracting and retaining top-quality talent has become a common plight for many organizations across the world.

In the cybersecurity space, however, this shortage can have debilitating effects.

With rapid advancements in technology, and the mounting sophistication and proliferation of cyber threats, large organizations, such as financial services institutions, require high caliber cybersecurity capabilities to avert financial and reputational repercussions.

While a shortage in cybersecurity talent is by no means universal, in certain geographies the talent pool can be incredibly shallow—and the war for that talent incredibly fierce.

Winning the fight will require creativity.

Not only will organizations have to cast a wider net in their recruitment efforts, but they must play a role in attracting and training people to enter the profession.

In this article, we explore ways to do this so organizations can keep pace in the rapidly evolving cybersecurity landscape.

What's behind the cybersecurity talent shortage?

To collectively resolve the cybersecurity talent shortage, it can be helpful to understand why it exists in the first place.

Naturally, part of the reason is due to the surge in global cyber attacks and data breaches. While there are many factors contributing to the increased incidence of attacks, at least some of the causes include misconfigurations, human error, and weak security management.

But a rapid rise in demand for talent is only one piece of a larger puzzle. The truth is, there are many reasons why organizations across the world can't seem to hire enough top-tier cybersecurity staff.

Insufficient educational programs

In many parts of the world, cybersecurity is a component of technically-focused college-level IT programs—and is treated as a skill-based course individuals can take after they earn their degree.

In some jurisdictions, you can obtain a standalone certification in cybersecurity, but it's not considered a university program in itself.

In countries where universities do offer cybersecurity programs—such as the United States, Canada, Brazil, Japan, and Australia—the availability of these programs is often limited to only a handful of institutions.

Additionally, promotion of those programs is all-too-often lackluster, with cybersecurity very rarely being effectively marketed as a legitimate career option.

Misperceptions about the industry

As cyber threats have evolved so, too, has cybersecurity—and, as a result, the awareness level around what this profession entails varies greatly.

Many senior leaders, for instance, still believe cybersecurity is primarily a highly technical profession, and aren't aware that it can also include many non-technical roles. In fact, effective cybersecurity teams are often a mix of members with technical, analytical, and soft skills. Recognizing this can dramatically broaden an organization's cybersecurity talent pool and make mid- and senior level recruiting much easier.

Cultural barriers

Misperceptions around cybersecurity impacts the number of people pursuing such careers as well as the types of people organizations hire. But these misperceptions are by no means universal and actually differ from country to country.

In Japan, for instance, most graduates join a company as a generalist, and work through different departments over several years before deciding on an area of specialization. In most cases, cybersecurity isn't included in this rotation, so individuals don't perceive it as a viable career option. Talent here is also more likely to see cybersecurity as "weird" or view cybersecurity professionals as the "bad guys".

As a result, technically-inclined people may opt to pursue jobs related to something like artificial intelligence, which has a safer reputation. In other areas, like Korea, people are less likely to apply for jobs they perceive to be outside of their skillsets.

So if their background is in a generalist IT role, for instance, they may see cybersecurity as something beyond their career track. People in Singapore, on the other hand, may be more open to exploring cybersecurity roles, because their country is home to many overseas Security Operations Centers (SOCs) and cybersecurity operations roles, and therefore offers greater exposure to the potential of this profession.

"Many senior leaders, for instance, still believe cybersecurity is primarily a highly technical profession, and aren't aware that it can also include many non-technical roles. "

Working conditions

In some jurisdictions, cybersecurity has a reputation for being a low-paying job with long hours and few opportunities for career advancement. In a recent Deloitte survey, 27% of respondents acknowledged that the cybersecurity profession lacks clearly-defined career paths, 23% said they lacked learning and development opportunities, and 30% felt compensation and incentive plans weren't keeping pace with the market.[1]

Recognizing this, a growing number of companies are taking strides to mitigate burnout in the profession, although certain jurisdictions are gaining better traction than others. In countries like Japan and the UK, employers are legally required to give employees paid time off for national holidays or health reasons.

In the United States, cybersecurity professionals may not receive paid time off—and may have to provide a doctor's note in the event of illness.

Gender inequality

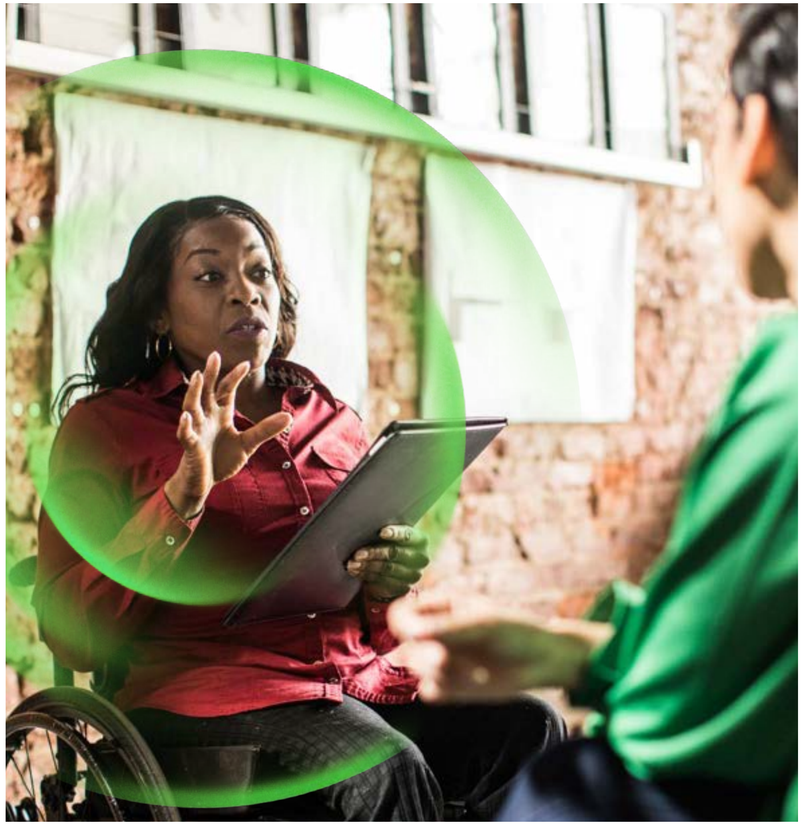
Like many Science, Technology, Engineering, and Math (STEM) workforces, cybersecurity is predominantly male dominated, resulting in a self-perpetuating gender gap.

Due to gender inequality in the field, many women drop out of STEM programs before ever entering the job market.

Of those who do go on to take STEM jobs, many see cybersecurity as unwelcoming rather than as a viable career path.

With only half the population considering cybersecurity as a profession, the talent pool remains limited.

Additionally, because the existing workforce only reflects one gender, any research done to attract diverse workers to the profession is often skewed.



Research done to attract diverse workers to the profession is often skewed.

Closing the gap

While many organizations across the globe are grappling to find adequate cybersecurity talent, a small fraction are beginning to differentiate themselves in the marketplace.

To join their ranks, organizations can employ a few different tactics.

Get more involved in academia

Right now, academia tends to treat cybersecurity as a supplemental skill—something you acquire after a degree—rather than a Tier 1 educational program.

To deepen the cybersecurity talent pool, this must change.

Organizations can support this effort by:

- providing worker retraining and a clear path to cybersecurity careers
- increasing the female presence in cybersecurity by collaborating with schools, universities, and recruiters
- working with educators to better align learning with industry skill needs, such as by sponsoring research chairs at universities, working with colleges and universities to develop curricula, or adding or augmenting cybersecurity courses
- encouraging cybersecurity professionals to teach in academia and get involved in the delivery of new educational programs so they can model what "real world" career paths look like

Broaden your horizons

Successful cybersecurity teams are strengthened when team members have diverse disciplinary backgrounds.

As such, it makes sense to broaden recruitment efforts and introduce cybersecurity to individuals who may not view it as a traditional career option.

To guide your efforts, it can be helpful to build well-rounded teams that include seven key cybersecurity personas (see p06 for more on these).

Not every persona requires an IT background or even a post-secondary education. In fact, if the passion is there—and if your organization is willing to provide the required training—post-secondary graduates with almost any degree can find an entry level job and go on to build a successful cybersecurity career.

Challenge misconceptions

If cultural barriers and misconceptions are preventing individuals from applying for cybersecurity roles in your region, it may be time to explore the root cause of those barriers and devise a marketing strategy to overcome them.

This will involve reflecting on the needs of the local talent pool, their perception of your business, and the talent narrative you're telling.

For instance, according to the Deloitte Global Gen Z and Millennial survey, 39% of Millennial workers and 36% of Gen Z workers say they value roles that allow for work/life balance.[2]

To meet these needs, organizations will have to also adopt the values of their workforce, integrate these values throughout the business and its operations, and highlight how their cybersecurity roles reflect them.

Meaningful work, a positive and trusting work environment, a commitment to effective management practices and behaviors, and opportunities for growth and development.

When you combine this with other benefits—such as meaningful work, a positive and trusting work environment, a commitment to effective management practices and behaviors, and opportunities for growth and development—it becomes easier to change cultural perceptions around cybersecurity and win over curious candidates.

Keep people moving

Cybersecurity has traditionally been seen as a somewhat monotonous line of work with few opportunities for career advancement.

One way to overcome this is by taking a page out of the SOC playbook.

In many large SOCs, people spend no more than two years in a particular role before they're moved to another function.

By offering individuals new opportunities every few years, sometimes in different parts of the world, organizations can keep their employees engaged and allow them to continually develop new skills, which increases job satisfaction and organizational loyalty.

Combining this tactic with things like job flexibility, skills training, stretch assignments, formal and informal mentorships, greater work/life balance, and competitive pay can help eradicate cybersecurity's poor reputation. win over curious candidates.

Explore new geographies

While some major cities struggle with talent shortages—particularly where large banking centers, technology hubs, and public sector organizations are located—there are countless smaller cities that have a wealth of idle talent.

By building capability in smaller suburban areas, organizations may find they have the pick of a wider talent pool.

The Seven Cyber Personas

Strategist
Provides cybersecurity management, direction, and advocacy

Advisor
Advises on the concept, design, and/or building of secure systems and networks

Defender
Supports, administers, and maintains the security of systems, data, and networks

Firefighter
Identifies, analyzes, and mitigates threats to internal systems, data, and networks

Hacker
Conducts specialized threat detection and deception activities to identify and mitigate cybersecurity risks

Scientist
Performs specialized analysis of threat intelligence, pattern analysis, and cryptographic and security information to improve security posture

Sleuth
Investigates cybersecurity events or crimes related to systems, networks, and digital evidence

Behind the curtain
How Deloitte attracts top cybersecurity talent

Like our Deloitte clients, Deloitte isn't immune to the global cybersecurity talent shortage.

Below are just a few ways Deloitte is putting recommendations into practice and building a strong global cybersecurity team.

Internship programs and sponsorships
In Australia, Deloitte partnered with the state government to sponsor a cyber academy.

Through this program, the government subsidizes approximately 40 university students each year to work with Deloitte and our clients, and acquire valuable hands-on cybersecurity experience.

The Netherlands offers a similar program, where student interns have an opportunity to learn about cybersecurity first-hand —and potentially land a job with Deloitte upon completion of their internship.

Professional training bootcamps
The Deloitte office in Brazil recently completed its second cybersecurity bootcamp.

Through this program, Deloitte Brazil provides cybersecurity training to a few hundred professionals.

Those that graduate in the top of the class are offered jobs at Deloitte, while the rest are equipped with the skills they need to launch successful cybersecurity careers at other companies.

Your work, your way
In Canada, we discovered the thing workers value most is flexibility, so we devised a program that allows them to decide whether they prefer a full-time office working arrangement, full-time remote arrangement, or a hybrid arrangement.

Cybersecurity roles are conducive to any of these arrangements.

Some of our cybersecurity positions rely on collaboration and problem solving, making them the perfect option for someone who loves a dynamic in-office experience.

Those who prefer to work from home, however, can also find a place on our team.

The path forward

Finding cybersecurity talent is challenging for many organizations right now —but, contrary to popular belief, the problem isn't only a talent shortage.

Rather, it's how organizations approach the talent search and how they're defining the ideal cybersecurity job candidate.

The talent pool of university graduates with IT backgrounds is shallow in many markets across the world, allowing those candidates to demand six-figure salaries.

But as we've outlined in this paper, the best cybersecurity teams are diverse cybersecurity teams—so while you still may need some members with IT backgrounds, the rest of the team may already be working within your organization (albeit in different functions) or be graduating from a different discipline.

Once you identify the range of candidates that can support your organization in its cybersecurity efforts, it's important to take note of what they need to realize personal fulfillment in the role and strive to offer them both competitive pay as well as a sense of purpose.

To learn more about how Deloitte can help you build effective cybersecurity teams, contact us.

Connect with us

Endnotes

1 *https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF*

2 *https://www2.deloitte.com/global/en/pages/about-deloitte/articles/genzmillennialsurvey.html*

Nick Seaver
Partner – Deloitte UK
Cyber and Strategic Risk

nseaver@deloitte.co.uk

Dinesh Santhiapillai
Partner – Deloitte Australia
Cyber and Strategic Risk

dsanthiapillai@deloitte.com.au

Steve Rampado
Partner – Deloitte Canada
Cyber and Strategic Risk

srampado@deloitte.ca

Eder de Abreu
Partner – Deloitte Brazil
Cyber and Strategic Risk

eabreu@deloitte.com

Ari Davies
Partner – Deloitte Japan
Cyber and Strategic Risk

ari.davies@tohmatsu.co.jp

Deloitte.