

SecurityCompass

Is There a Cybersecurity Skills Shortage?



On Sep. 5, 2020, CNBC released a news brief that **over 4 million cybersecurity roles are required globally to close the skills gap** with over half a million required in the United States alone.

While some may consider this to be news, those within the industry believe that it's an existing situation being made worse with the onset of COVID.



Cybersecurity Skills Gap

4.07 MILLION PROFESSIONALS

In April 2019, the global cybersecurity workforce was estimated to be around 2.08 million professionals [as per a study by \(ISC\)²](#). To fill the skills gap in cybersecurity, there's a need of 4.07 million additional professionals.

Harvard Business review also quotes “the majority of chief information security officers (CISOs) around the world are worried about the cybersecurity skills gap, with 58% of CISOs believing the problem of not having an expert cyber staff will worsen.”

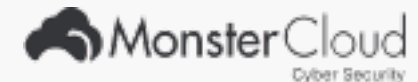
So what's made it worse during COVID? A recent [\(ISC\)²](#) study indicated that cybersecurity incidents have escalated after moving to remote work as per 23% of the organizations. Some of them have experienced a twofold rise in these incidents. Compound this startling statistic with 47% of respondents indicating that they “have been taken off some or all of their typical security duties to assist with other IT-related tasks, such as equipping a mobile workforce.”



23% OF ORGANIZATIONS reported that cybersecurity incidents have escalated after moving to remote work.

The lack of skilled and appropriate individuals is having an impact during COVID:

1. The [FBI](#) recently reported that the number of complaints about cyberattacks to their Cyber Division ranged between 3,000 and 4,000 each day - a major jump from prior to the COVID-19 pandemic when about 1,000 complaints were received daily.
2. [Interpol's](#) "assessment of the impact of COVID-19 on cybercrime has shown a significant target shift from individuals and small businesses to major corporations, governments and critical infrastructure."
3. [Zohar Pinhasi](#), a cyber counter-terrorism expert and founder of the cybersecurity firm MonsterCloud, "reports that his cyber security firm, MonsterCloud, has had an 800 percent increase in calls since the virus forced many Americans to work from home. "
4. Studies indicate it can take up to six months to hire new cybersecurity engineers. In the meantime underskilled practitioners are managing security as organizations use existing staff to fill gaps.
5. Cybersecurity is complex and there is often an extensive security specific tool set that staff don't know or understand (the [average enterprise organization has 75](#)).



**THE AVERAGE
ENTERPRISE HAS
75 CYBERSECURITY
TOOLS**

What is an organization to do when faced with such a significant challenge

With little foreseeable change happening in the labor market the only solution that organizations have is to automate:

1. Tools exist that enable developers to consistently implement security and compliance standards into software so that it can be tracked by an organization. These tools allow security experts to focus on high value organization solutions.
2. These same solutions need to ensure that all developers have access to the same security information and requirements via on demand training. Security experts rarely have time to train individuals developers – and developers don't have time to sit through training they may not use for weeks.
3. These solutions need to eliminate as many software vulnerabilities as possible so that developers don't spend time repetitively working through the very same piece of code. With limited staff organizations need to use developers as effectively as possible.





Can Balanced Development Automation solutions help

The future of the business relies on being digital - and software being deployed better be secure and protect privacy! Organizations might be *fast and risky* by relying on testing, scanning, and audits, then fixing code. Or perhaps, they're *slow and safe*, producing threat models, risk assessments, and security requirements with scarce and expensive experts.

However from the statistics we've provided above organizations are likely moving in the fast and risky direction. But what if organizations could **go fast and safe**, proactively building in security and compliance at scale?

SD ELEMENTS

the world's first **Balanced Development Automation** solution:



1
Gathers info about your project, either from existing data sources or a configurable survey.



2
It then assigns a risk classification, and a powerful logic engine crawls our expert content library for relevant security and compliance risks. Accordingly, it suggests countermeasures.



3
Based on that, DevOps teams receive detailed requirements, code samples and short, relevant training modules right in their issue trackers, such as Jira.



4
Next, it imports results from your code scanning tools to automatically validate which security activities were completed and which are outstanding.



5
It instantly produces detailed reports so your teams know exactly where their risk lies.

A **Balanced Development Automation solution like SD Elements assists organizations in coping with the lack of individuals with cybersecurity skills.**

Go Fast. Stay Safe.™

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt Balanced Development Automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on how organizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter [@securitycompass](#) or visit them at [securitycompass.com](#) to learn more.

1.888.777.2211

info@securitycompass.com

www.securitycompass.com

 @SECURITYCOMPASS

 SECURITY COMPASS

SecurityCompass

OFFICES

GLOBAL HEADQUARTERS

1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO

390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY

621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA

995 Market Street
2nd Floor
San Francisco, CA
USA 94103

INDIA

#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001