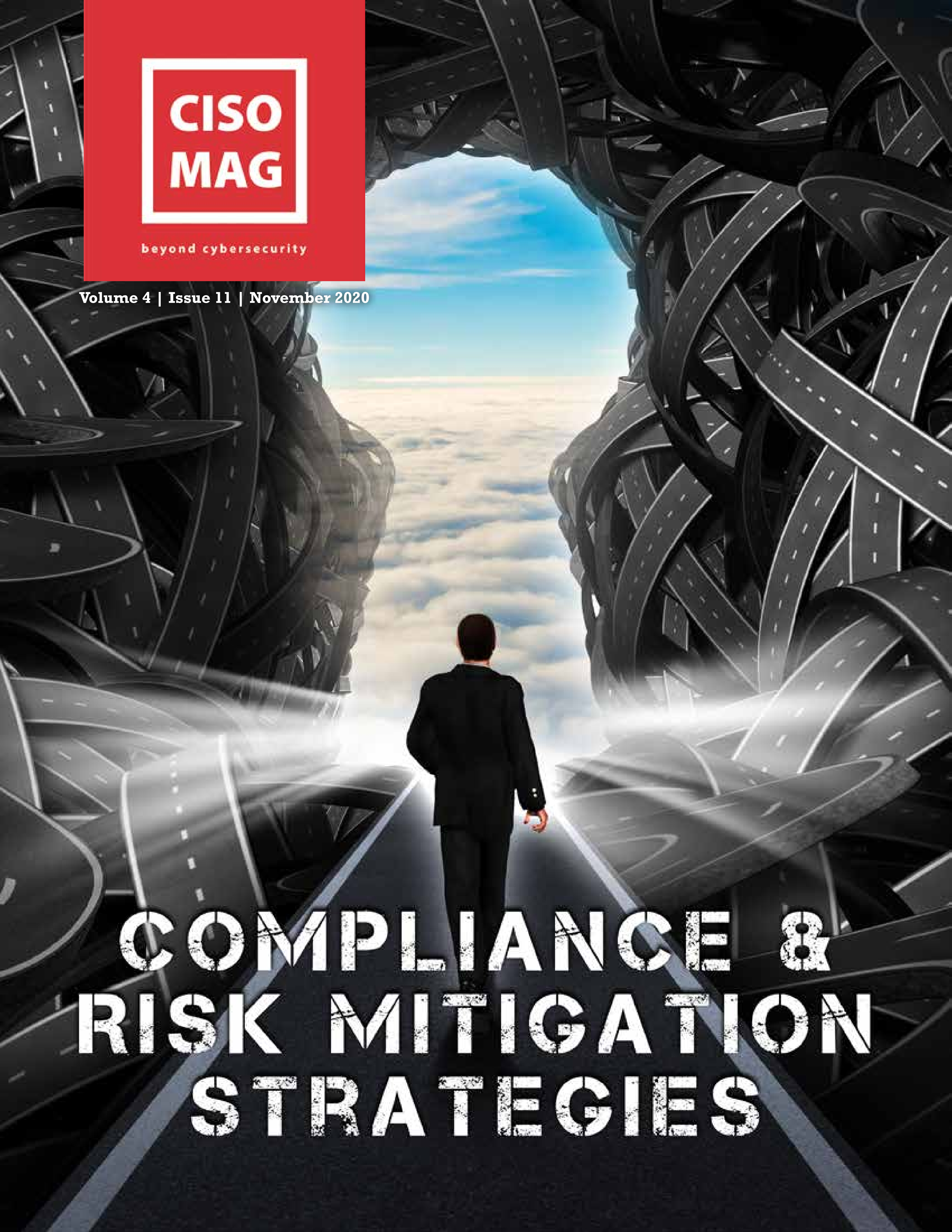
CISO MAG

beyond cybersecurity

Volume 4 | Issue 11 | November 2020



COMPLIANCE & RISK MITIGATION STRATEGIES

I THINK IT’S EXTREMELY UNPRODUCTIVE TO HAVE INDIVIDUAL STATE PRIVACY STANDARDS

INTERVIEW

ARMISTEAD WHITNEY
FOUNDER AND CEO
APPTEGA

Armistead Whitney is the **Founder and CEO of Apptega**, the software platform helping businesses around the world build, manage and report their cybersecurity programs. He has over 25 years of experience in creating and leading enterprises in the security, software and Internet industries including raising over $75 million in venture capital and participating in a successful IPO. His passion is developing creative go-to-market business strategies, launching new products, implementing predictable metrics-driven sales models, and fostering team culture in industries ripe for change.

In an exclusive interaction with **Augustin Kurian from *CISO MAG***, Armistead talks about Industry 4.0, its cybersecurity implications, traditional multi-layered defense techniques, and the cybersecurity skill gap.

Industry 4.0 is progressing at a very fast pace and creating disruptive challenges in the day-to-day life of mankind. What lies behind this phenomenon — the fourth industrial revolution — and what will be its impact on the cybersecurity landscape?

The transfer of power from humans to software, devices, and robotics in manufacturing in a fourth industrial revolution world will have major impacts on the cybersecurity landscape. IIoT (Industrial Internet of Things) devices often exist across flat networks that are unprotected, giving threat actors multiple entry points to penetrate them. IIoT ecosystems that include prized IP and commerce (transactions) will be at the highest risk for hackers to focus on. The impact of this risk will likely include the creation of new regulations and standards to protect businesses and global economies, software-driven security solutions that operate in real-time and can monitor the entire vertical IIoT system, and the need for more interoperability between security products that can work more seamlessly together across the entire network.

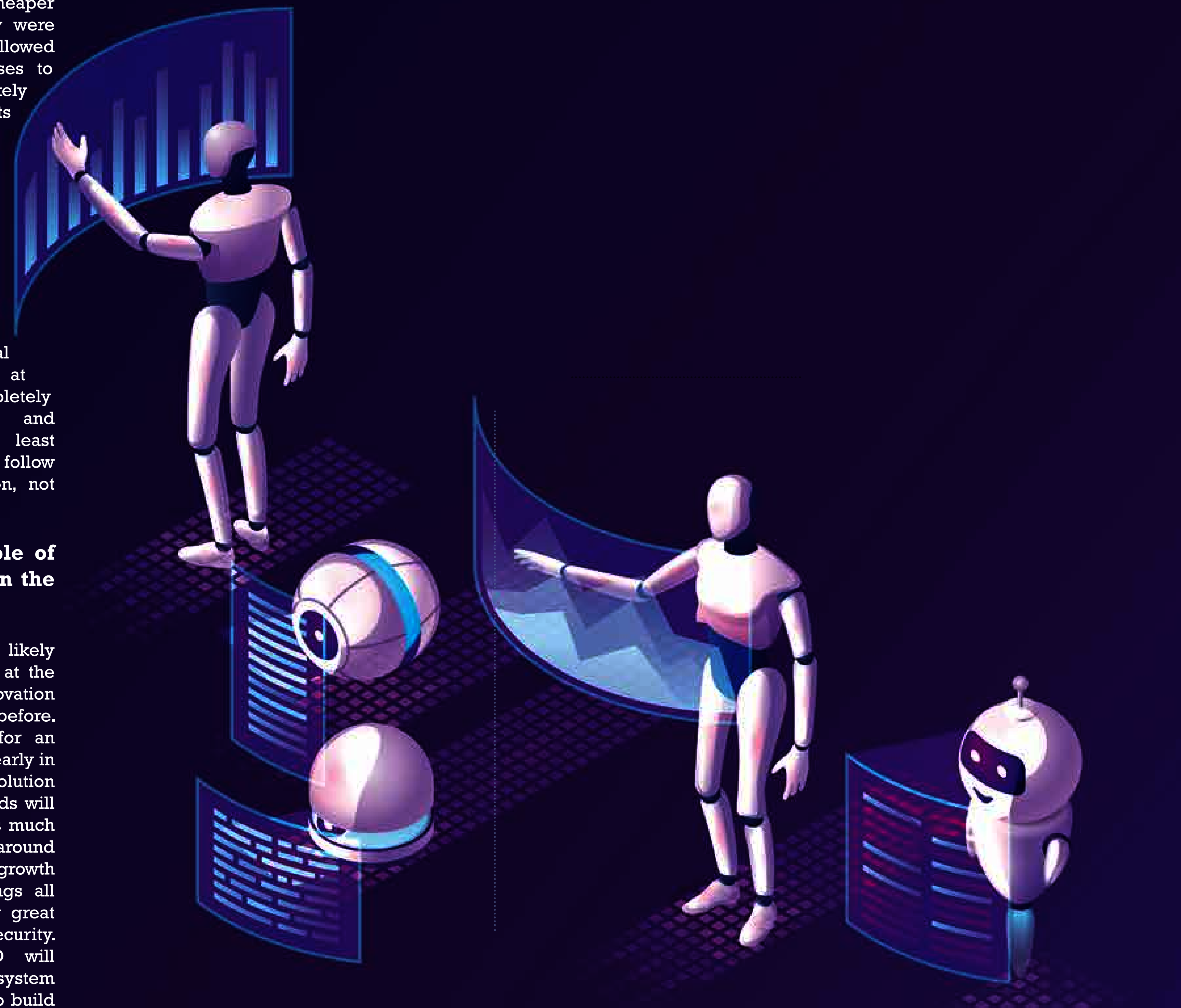
> As technology is embraced in the wider mainstream market, cybersecurity became an essential element to maintain the speed of the revolution. As we look to Industry 4.0 adoption, cybersecurity will likely be more at the forefront than in any previous industrial revolution, but not at the risk of completely stifling innovation and monetization, at least early on. It tends to follow disruptive innovation, not lead it.

According to a study on good practices for IoT security, and smart manufacturing, cybersecurity is a key enabler for Industry 4.0 adoption. What are your thoughts on that? Do you believe the global approach towards cybersecurity has changed, and a model of security-by-design is standard?

I'm not convinced that cybersecurity is a key enabler for Industry 4.0 adoption. If history proves correct, we can look back to the Third Industrial Revolution — the invention and proliferation of networks, computers and then the Internet itself with all of the breakthroughs replacing human, manual labor in some way — make things better/faster/cheaper as the cliche goes — which fundamentally were created by scientists and engineers first followed by entrepreneurs who developed businesses to capitalize on those technologies. It's unlikely these two essential stakeholders — scientists and entrepreneurs — took a "cybersecurity first" approach. Rather, as technology is embraced in the wider mainstream market, cybersecurity became an essential element to maintain the speed of the revolution. As we look to Industry 4.0 adoption, cybersecurity will likely be more at the forefront than in any previous industrial revolution, but not at the risk of completely stifling innovation and monetization, at least early on. It tends to follow disruptive innovation, not lead it.

How will the role of a CISO evolve in the Industry 4.0?

First, the CISO will likely have a bigger seat at the table early in the innovation curve than ever before. A lot is at stake for an organization to win early in a new industrial revolution and CEOs and Boards will want to eliminate as much risk as possible around their IP, revenue growth and brands — things all at stake with either great or poor cybersecurity. Second, the CISO will have a daunting task to sort through an ecosystem of 5,000+ cybersecurity tools and solutions to build the right ecosystem with as few vendors as possible. Interoperability between products needs to improve significantly to make this easier for the CISO. We're already seeing several leading brands partnering together to bring more "total solutions" to the market, but that needs to happen much more and on a larger scale. And not just leading brands, but emerging



brands and start-ups need to participate as well. CISOs are caring less and less about working with the biggest providers, and more about the stitching that can occur between multiple providers to make vendor management, implementation and investments much more favorable.

Regulators around the world are taking notice and implementing new controls for cyber risk to address the growing threat to enterprises. In recent years, there has been a paradigm shift in the way attackers are exploiting the source, behavior, vector, and motives. Even COVID-19 changed the dynamics of cybersecurity. Is traditional multilayered defense that enterprises already have adequate to protect against attackers?

Even before COVID-19, many enterprises were finding that they didn't have good cybersecurity hygiene, even despite multilayered defense systems, due to a number of issues like short-staffed cybersecurity teams, keeping up the increase in enterprise apps, and moving more infrastructure to the cloud. With the average enterprise using 50+ security-specific tools to protect data and intellectual property, understaffed security teams are forced to manage tool sets they don't know or understand how to fully utilize.

The pandemic has highlighted the importance of strong cybersecurity systems, especially as a large portion of the workforce adapts to working from home and stretches the boundaries of distributed networks.

According to a research, 91% of all enterprises follow a cybersecurity framework, which equates to 400,000 companies and over 2.8 million cybersecurity professionals are searching for ways to find the right vendors. There appears to be a need for a B2B ecommerce marketplace dedicated solely to cybersecurity and compliance. How is Apptega helping enterprises on this specific front?

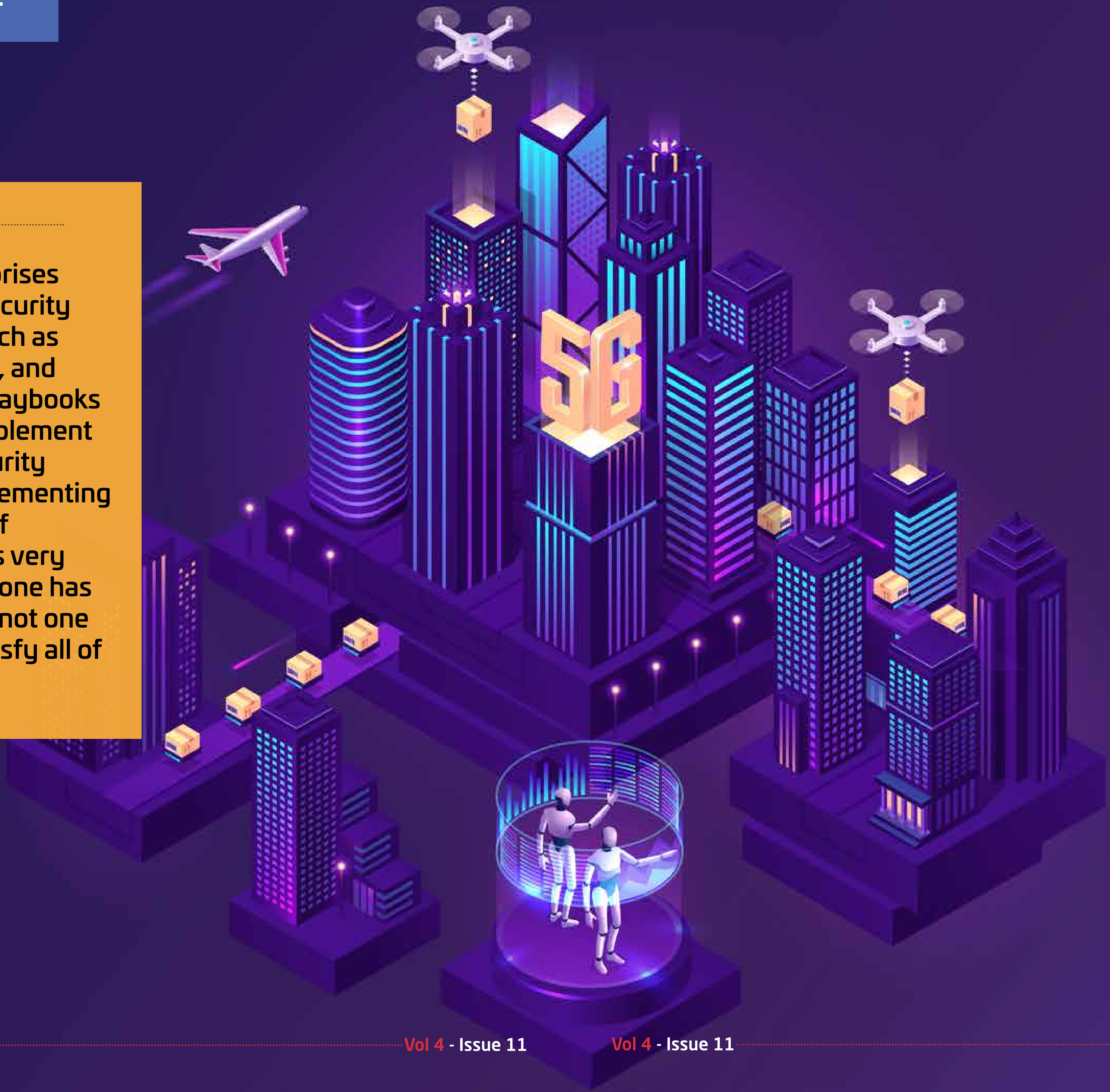
As more enterprises turn to cybersecurity frameworks such as SOC 2, PCI, ISO, and NIST as their playbooks to build and implement their cybersecurity programs, implementing the hundreds of requirements is very complex. PCI alone has over 250+ and not one vendor can satisfy all of them. So, CISOs and their teams in IT are forced to navigate 5,000+ security vendors to find the best solutions and none of them talk to each other. Traditional channels for buying security are very cumbersome and inefficient and include sifting through hundreds of choices on Google, attending trade shows and conferences (not possible today with COVID), or dealing with constant cold calls and cold emails from security company sales reps.

CyberXchange by Apptega maps cybersecurity products and services to exact framework requirements on the subcontrol level enabling a buyer to easily search, self-educate, compare pricing, and purchase solutions all in one place matched to their framework in a way that's simple and easy to navigate. The underlying technology in CyberXchange is a proprietary mapping engine with AI, called Harmony. Harmony pulls in the criteria and configurations of thousands of security products and services and maps it to 10,000+ security framework controls and categories. It also contains a predictive model that ingests vendor data and assigns it to the right search results. Users get super accurate search results and insights. CyberXchange also shows how a particular solution maps across multiple requirements in a framework, which helps eliminate vendor overlap and redundancy and improves a company's ROI on its cybersecurity investments.

From a cybersecurity standpoint there are several cybersecurity guidelines and compliance norms across different countries and regions, like SOC 2, PCI, HIPAA, NIST, CMMC, CCPA, and GDPR. Do you believe there should be a standard global cybersecurity compliance instead of multiple ones?

For the foreseeable future, we'll continue to see multiple industry-specific cybersecurity compliance standards like SOC 2 (cloud), HIPAA (healthcare), and PCI (retail/ecommerce) applying to the U.S. companies. However, privacy may be a different story. With GDPR being the new European privacy standard widely adopted globally and CCPA being out for many months to protect California consumers, it's likely other states in the U.S. will follow suit and

> As more enterprises turn to cybersecurity frameworks such as SOC 2, PCI, ISO, and NIST as their playbooks to build and implement their cybersecurity programs, implementing the hundreds of requirements is very complex. PCI alone has over 250+ and not one vendor can satisfy all of them.

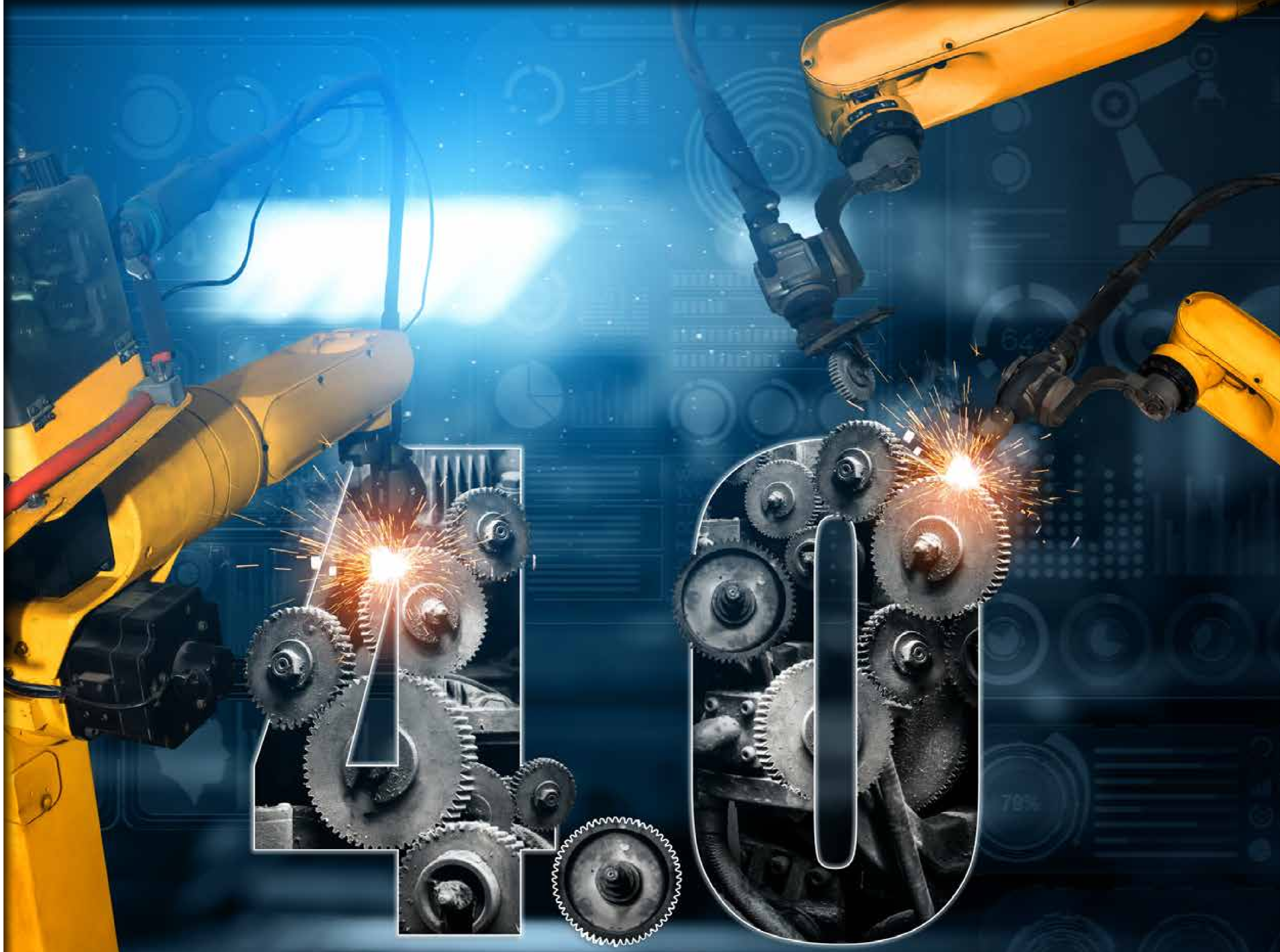


push ahead with their own privacy standards. I think it's extremely unproductive to have individual state privacy standards. The amount of effort for companies of all sizes to manage 50+ compliance standards for doing business with consumers across state lines is unimaginable. I believe one national compliance standard for consumer protection makes the most sense and is inevitable. However, given that it's an election year and the impact of COVID, any initiatives to create a national privacy standard are likely paused for now. It's a real struggle for security and IT professionals to implement solutions to satisfy the hundreds of controls mandated by the standards. Translating the control requirements to a specific product is not an easy task and it ends up creating overlaps, excessive spending, and vendor overload.

By 2022, it is estimated that 1.8 million new cyber experts will be needed globally. Inclusivity including gender diversity, racial diversity, and neurodiversity is usually pointed to as a leading strategy, but the problem persists. What is your take on that, and what solutions do you suggest?

There is a huge lack of cybersecurity talent in the market, exceeding 1 million open jobs. Interestingly, cybersecurity is one of the highest paying jobs in IT — averaging well into the six figures annually, and it's an industry that will continue to grow for many years. Yet, it's been very challenging to fill the gap. One issue is the amount of training it takes to learn the cybersecurity trade. All the school course work and degrees in the world are no substitute for real-world experience. It can take years to achieve the knowledge and experience needed to be great at it. With the average new worker switching jobs every two years, continuity is also an issue. I believe the solution lies in education, government, and private enterprises working together to foster young career seekers to focus on cybersecurity. A great example of this is the Cybersecurity Talent Initiative sponsored by Workday, Mastercard, and Microsoft. It is an initiative (https://cybertalentinitiative.org/) where students get up to $75,000 in student loan forgiveness to get into cybersecurity, and get real world experience. In addition, I believe there is an underserved pool of gender diverse, racially diverse, and neurodiverse workers that need new channels opened for them to enter cybersecurity through programs similar to the Cybersecurity Talent Initiative 🔒

Augustin Kurian is part of the editorial team at CISO MAG and writes interviews and features.



Disclaimer: CISO MAG did not evaluate/test the products mentioned in this article, nor does it endorse any of the claims made by the writer. The facts, opinions, and language in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same. CISO MAG does not guarantee the satisfactory performance of the products mentioned in this article.