info security

STRATEGY | INSIGHT | TECHNOLOGY

Unchaining Cybersecurity Research?

The US attempts to prevent the prosecution of white hat hackers

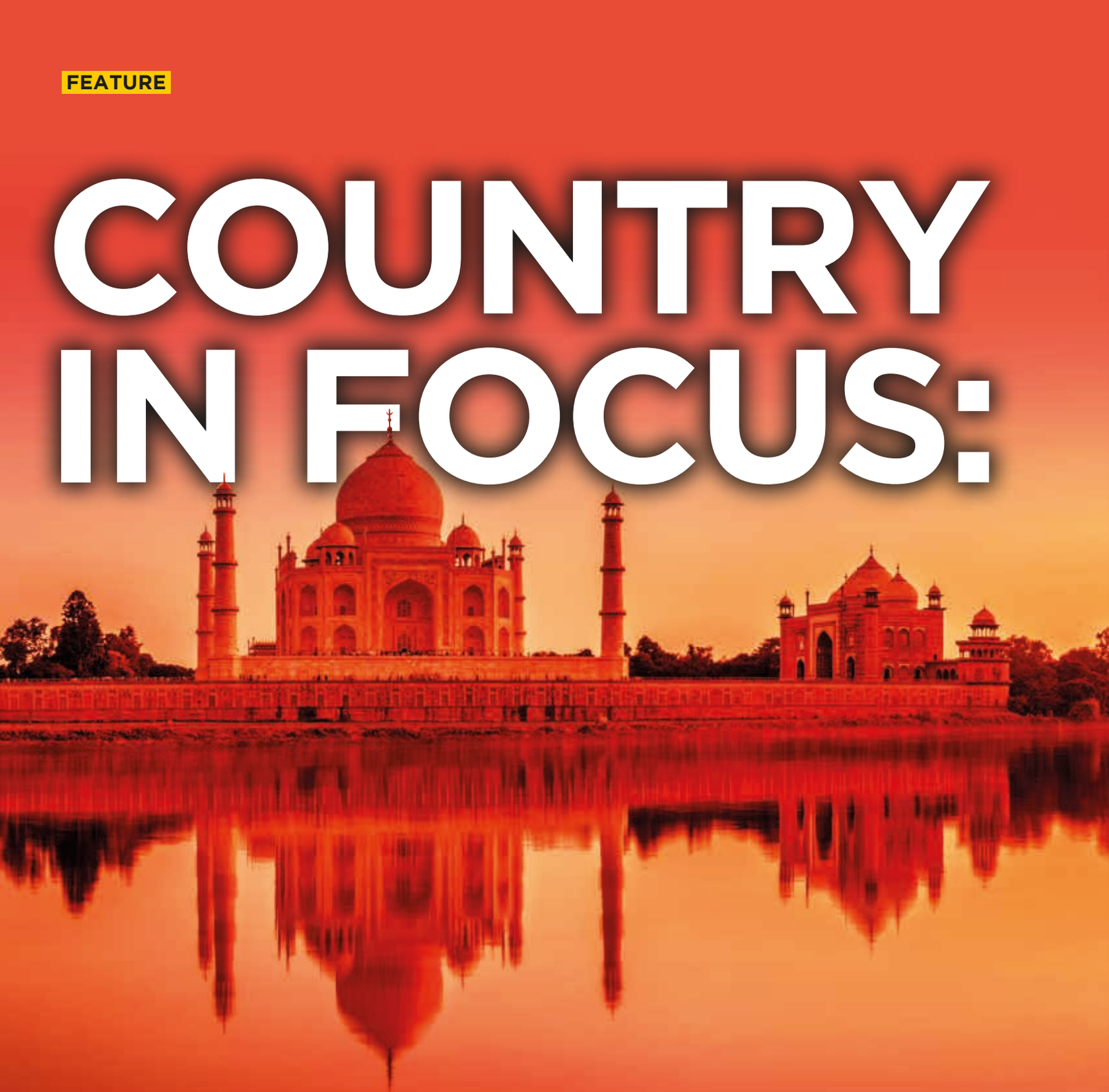
Q3, 2022 / Volume 19 / Issue 3

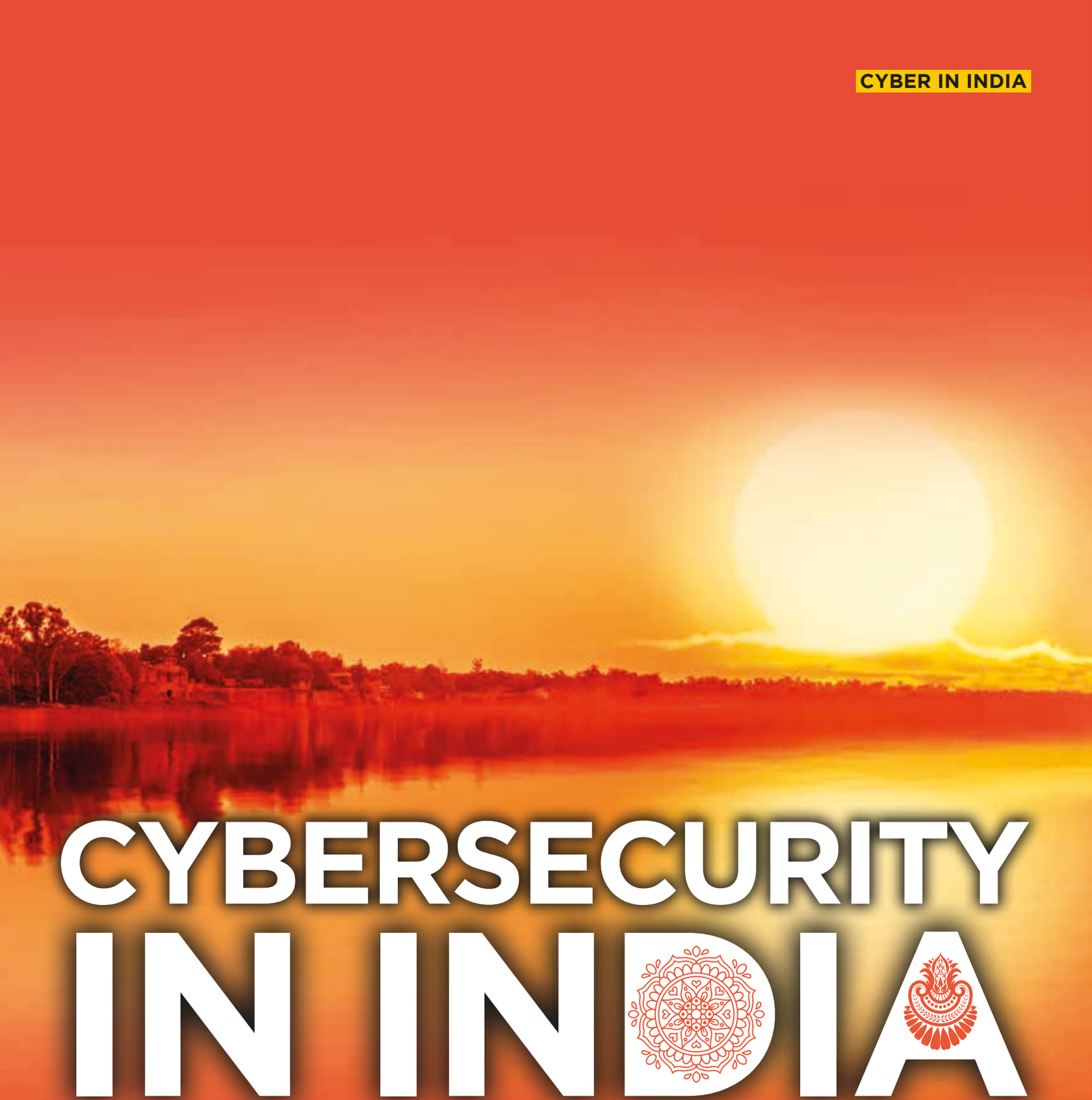
AN AGE OLD QUESTION
Exploring age diversity in cybersecurity

IN-FLIGHT CYBER-ATTACKS
Is this dystopian scenario plausible?

INDIA IN FOCUS
Cyber challenges in this critical economy

COUNTRY IN FOCUS:





CYBERSECURITY IN INDIA

Shweta investigates the state of cybersecurity in one of the fastest growing economies in the world, India. What are the major cyber threats and challenges in this key geopolitical region?

Cybersecurity issues are truly global and the strongest economic nations are often hit the hardest. India is the fifth largest economy in the world, and also is in the top five nations in terms of the number of victims of internet crime, with only Canada, the UK and the US logging more victims, according to the US FBI's Internet Crime Report 2021. The FBI findings state that India reported 3131 victims of cybercrime. This has increased from the 2022 report, which showed 2930 victims logged.

Two of the most comment types of cyber-attack seen in India are endpoint attacks (especially ransomware) and credential theft.

Shomiran Das Gupta, CEO at NetMonastery, says: "India has seen lots of direct endpoint attacks [aka] ransomware. This is the case everywhere, but in India, ransomware is causing maximal damage. The next thing we see is credential theft, and that credential theft is being very smartly used for stealing secrets and money at the corporate level."

Indian Organization Preparedness

Gaurav Shukla, cyber leader at Deloitte India, says that "in India, all mature organizations are aware of the need for a robust cybersecurity platform and ability to report and take some action."

Despite this, the typical response of companies in the event of an attack is delay and denial before finally accepting something "might" be amiss in their security framework. Of course, that might be due to the differential maturity level of organizations, ranging from still defining frameworks and undertaking ad hoc reporting to having security operations centers (SOCs) and security information and event management (SIEM) in place.

That needs to change. When regulated sectors like finance and banking can attain a high maturity level in terms of tool adoption, strategy and frameworks, why not the rest? Also, we must remember that intruders are not differentiating between their targets based on size or industry: they're all looking for vulnerabilities to exploit.

> ***"In India, all mature organizations are aware of the need for a robust cybersecurity platform and ability to report and take some action"***

Atul Gupta, leader, cyber security and digital trust at KPMG India, agrees, noting that "the key cyber threats are emerging in the form of large scale disruptions through ransomware attacks and mass level of data extraction through multiple digital channels."

Endpoint attacks seem the most effective way to intrude on any network because they are the most vulnerable link in the security chain. Even before the COVID-19 pandemic accelerated the pace of digitization, executives were using their smartphones and personal laptops to log in to their work accounts. This is often without the security basics in place, such as strong passwords.

A Kaspersky survey published in October 2020 revealed that only 17% of Indians were using password managers. Another study by LocalCircles in 2021 found that one in three Indians stored their banking passwords in emails, mobiles or PCs. Add into the mix the fact that the most favorite password of Indians is 'password,' and you have a disaster waiting to unfold.

This brings us to two questions. Are organizations equipped enough? And is the intent to protect private data there?

Traditionally, Indians are not very particular about data privacy and protection. As Dr Burzin Bharuch, advisor and cybersecurity trainer, EY India, points out, "We don't think twice about collecting or providing our critical private data like name, phone number, address, person to visit, etc. openly on registers upon entry to offices. Anyone could click a photo with their smartphones and have critical data in their possession."

We can come to the intent later as it is subjective and open to discussion. However, a string of successful breaches makes it clear that organizations are ill-equipped to deal with the accelerated barrage of cyber-attacks. Players at every level – from the front desk to the boardroom – need to accept their responsibility to improve security and privacy.

Past events involving the Kudankulam Nuclear Power Plant and the Mumbai Blackout may be the poster cyber incidents in India, but multiple attacks are being continuously detected. For example, the Indian Computer Emergency Response Team (CERT-In) has reported more than 200,000 cybersecurity incidents in the first two months of 2022, while the Indian Petroleum Refineries network witnessed over 300,000 attacks between October 2020 and April 2021.

As threats become more complicated in severity because of the sophisticated techniques used by attackers, outdated tools and knee-jerk reactions can no longer suffice. Leaders within government and private enterprises must continuously monitor the current global threat landscape and create a strategy to proactively identify weaknesses, augment human skills and defend against threats.

Das Gupta says: "Knowing how to use [the tools] and [having] the vision of figuring out what to protect against is important. Nobody in the world can protect themselves against everything. You have to choose your battles and plan against those vulnerabilities."

Indian Government Efforts

Besides the general cyber-attacks on the ecosystem, governments need to deal with nation-state actors, and India is no exception. The positive is that the Indian government is gearing up in the right direction through the CERT-In under the Ministry of Electronics and Information Technology (MeitY).

CERT-In is the functional organization for securing Indian cyberspace. It monitors Indian cyberspace to issue alerts and warnings for imminent attacks. The keyword here is 'functional,' as many other agencies and ministries are involved too.

The National Security Council Secretariat (NSCS) is the apex agency responsible for India's political, economic, energy and strategic security concerns. Then there is the National Information Board (NIB), headed by the National Security Adviser (NSA), which is responsible for enunciating the national policy on information security and coordinating all aspects of information security governance in the country.

The National Cyber Coordination Center (NCCC) was set up by CERT-

In and functions under NIB. It designs cybercrime prevention strategies, provides cybercrime investigation training and reviews outdated laws, among other tasks.

The National Critical Information Infrastructure Protection Centre (NCIIPC) is a specialized body created by the Department of Information Technology to protect India's critical information infrastructure. Finally, the National Crisis Management Committee (NCMC) deals with national crises arising from focused cyber-attacks.

As well as these specialist agencies, the Indian Ministry of Home Affairs, the Ministry of Defense, the Ministry of External Affairs and the National Technical Research Organization are all directly involved in monitoring and maintaining cybersecurity in the country.

It's clear that the Indian cybersecurity ecosystem is fragmented and needs a more centralized and streamlined effort to handle the looming threat of cyber-attacks.

Encouragingly, to boost cyber preparedness, CERT-In issued blanket guidelines for all industries in April 2022, which came into effect from June 2022. Businesses had a lot of concern about the six-hour incident reporting timeframe, but as Gaurav Shukla points out, "through these guidelines, the government wants [businesses] to look inward at their overall maturity level, including security incident and event identification, management and reporting processes."

To effectively deal with cyber-attacks, organizations need to embrace security and privacy by design. However, that's not possible without being resilient by design. CERT-In guidelines are nothing but a nudge towards setting up the baseline above which all entities must operate to be resilient.

> ***"The government wants [businesses] to look inward at their overall maturity level"***

Global Skills Shortage

The march towards the desired level of cyber maturity across the board requires the availability of the necessary cybersecurity workforce, which is in significantly lower supply than required.

As Gupta points out, the "challenge of skill availability continues to be a concern area, specifically to effectively address cyber risk across rapidly adopted new age digital technologies (cloud, mobile, connected devices/machines, remote working, etc.)." The solution to this issue is multifaceted.

Dr Burzin believes that "we need to catch them really young and start teaching them cyber hygiene from grade four or five." This preparation will produce the requisite cybersecurity workforce for the future. But what about the people we need right now?

It seems intuitive for the government to intervene and introduce more courses at college level. However, that alone is not enough. Organizations need to invest in training and retraining their cybersecurity workforce. As Das Gupta points out, "cybersecurity changes every moment. You aren't able to write practices to engineer solutions. [And] because you cannot do that, you can only get trained to a certain level and then from that point on you learn from your experiences."

Gupta notes that organizations can take a two-pronged approach to solve the immediate skills shortage. One, expand their talent pool by recruiting non-tech employees who can provide support in designing strategies and processes. Two, get more involved with on-campus training and education. For example, they can invite students for internships and summer training. Senior executives can also volunteer to take cybersecurity courses that attract the right talent to the fold.

Future of Indian Cybersecurity

Despite the challenges, the future of the Indian cybersecurity space looks bright because businesses are aware of the need for cybersecurity within their organizations and the government is set to pull all organizations up to a minimum maturity level. The right technologies and indigenous skills are also available, if harnessed in the right way. All that is needed is intent and focus END