# Cybersecurity landscape evolves with rising threats and new strategies



Experts predict significant transformations in cybersecurity practices as the landscape evolves to combat the staggering estimated loss of nearly $8 trillion annually due to compromised cybersecurity, as outlined in a report by McKinsey. A discussion held at the Cybersecurity Centre of Excellence (CCoE) in the city on Friday highlighted the pressing need for large corporations and end-users to employ "the right tools" to mitigate various internet threats.

This event saw participation from officials at the Data Security Council of India (DSCI) as well as representatives from multiple cloud computing and cybersecurity firms. Sriram Birudavolu, CEO of CCoE, emphasized the market opportunity within cybersecurity, estimating it to be between $2 to $3 trillion. He urged companies to establish dedicated Security Operations Centres (SOCs) to proactively defend against cyber threats. Drawing an analogy between cybersecurity and the human immune system, he stated: "Just like how our immunity protects our body 24x7, cybersecurity should also protect our data at all times."

In a troubling trend, Lalit Mohan S, chief product officer at Seqrite, reported that Telangana witnessed the highest malware attack rates last year, which rose from 12% to 15% in 2023. In response to this escalating danger, Seqrite and QuickHeal introduced an initiative called Antifraud.ai aimed at consumer protection. This mobile application provides users with real-time notifications to detect potential threats.

Kotilingeshwara Rao Vudhari, senior vice-president of Cloud4C, expounded on essential components of future SOCs, stating that they must leverage artificial intelligence and machine learning to effectively assess threats and analyse cyber incidents. Across the discussion, experts concurred that cybersecurity must be treated as a "fundamental aspect of digital infrastructure rather than an afterthought." Birudavolu reiterated this sentiment, saying, "Security and privacy should both be design and default."

Chandrashekhar Sharma, director of CtrlS, highlighted the necessity for a comprehensive approach that incorporates "vulnerability assessment, security orchestration, and automation" to address the growing threat of cybercrime. He articulated that a holistic approach is mandatory to safeguard data, insisting it is vital to "predict new threats and adapt to them." Sharma further likened cybersecurity to oxygen, noting that while it is often invisible, it becomes critically important at the moment it is compromised.

The discussion also touched on the concept of 'zero trust', which has become a focal point among cybersecurity professionals amidst the rise of diverse threats. Sai Aditya, enterprise information security officer at Reckitt, articulated the need for a systematic reevaluation of trust protocols, stating, "Zero trust is not merely a tool; it's a philosophy that eliminates implicit trust between devices, networks, and individuals." He stressed the importance of continuously scrutinizing website reputations and traffic patterns.

Aditya further stated, "Organisations need to move beyond traditional security approaches," advocating for an emphasis on security assessments aligned with business priorities rather than relying on immediate fixes. He concluded that developing cyber maturity is essential, underscoring that companies must adopt a methodical, zero-trust approach in the current threat environment to ensure robust cybersecurity practices.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://it.telangana.gov.in/initiatives/cybersecurity-centre-of-excellence/> - Corroborates the existence and objectives of the Cybersecurity Centre of Excellence (CCoE) in Hyderabad, including its role in innovation, entrepreneurship, and capability building in cybersecurity and privacy.
2. <https://ccoe.dsci.in> - Provides details on the CCoE's vision, mission, and the five main pillars of the ecosystem, including industry, government, academia, user groups, and collaborations with other industry bodies.
3. <https://it.telangana.gov.in/initiatives/cybersecurity-centre-of-excellence/> - Supports the involvement of officials from the Data Security Council of India (DSCI) and the role of CCoE in hosting events and initiatives.
4. <https://niccindia.com/ccoe-benefits/> - Outlines the comprehensive education, hands-on training, cutting-edge research, and industry collaboration aspects of a Cybersecurity Centre of Excellence, aligning with the discussion on establishing dedicated Security Operations Centres (SOCs).
5. <https://niccindia.com/ccoe-benefits/> - Details the importance of vulnerability assessment, security orchestration, and automation in addressing cyber threats, as highlighted by Chandrashekhar Sharma.
6. <https://it.telangana.gov.in/initiatives/cybersecurity-centre-of-excellence/> - Supports the emphasis on treating cybersecurity as a fundamental aspect of digital infrastructure rather than an afterthought, as reiterated by Sriram Birudavolu.
7. <https://ccoe.dsci.in> - Corroborates the need for a holistic approach incorporating various components to address growing cyber threats and the importance of predicting new threats and adapting to them.
8. <https://niccindia.com/ccoe-benefits/> - Highlights the necessity of a comprehensive approach to cybersecurity, including the use of artificial intelligence and machine learning in future SOCs, as discussed by Kotilingeshwara Rao Vudhari.
9. <https://it.telangana.gov.in/initiatives/cybersecurity-centre-of-excellence/> - Supports the concept of 'zero trust' as a philosophy in cybersecurity, emphasizing the elimination of implicit trust between devices, networks, and individuals, as articulated by Sai Aditya.
10. <https://niccindia.com/ccoe-benefits/> - Underlines the importance of continuous scrutiny of website reputations and traffic patterns, and the need for organisations to move beyond traditional security approaches, aligning with Aditya's advocacy for a zero-trust approach.
11. <https://news.google.com/rss/articles/CBMiugFBVV95cUxNVkVNR05YY3pDUFNIdEJiTWtjZUFnTl9uN2dlVi1CSUJLSVlBSVB1SzRBZDRUMGZJMDlEQ1VfOUpjTUtMRWlENjJyRHI0eFJlbEVqcnFDTDBmYWZ2cGRiZTIxTUdHQ21EY3VjMXNJSlZtYlFuV08wME9pUzZZWGFPMUpiSFgzenBDYVEyd0lxd0pQd1RUQnRYWTNuRXlHZWVjekFfU25GS25Ya0VPTXU2RV9oMUltWW5FUVHSAb8BQVVfeXFMUFRFeDFfVDVGM0l6MHFDSlI2c3pWYzNRV3VJSnlESE4yOVJzS0p6S2JBR0NZdG1ZNnYtSzNEN0xqYWl5cVFQOHU1alkyMHFycFhWczF4MUM5NHdTc0t0OXZHazZ1azFkd2FGNHBxU21QSjNaVW1JT3ZYX0VoN1JxZ3hORXVhT05JVlpTQkpTbS1ZVnhQTVpFbjM1ekl5UnFsanVWb1V2Mkl4bkJfQzBjRmdUSVdaNDZUQW00c0NQY0U?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data