Cybersecurity Management and Reporting

The cybersecurity practices at Infosys have evolved to look beyond compliance. The comprehensive cybersecurity metrics program has been contributing to the continuous improvement of the existing security practices and integration of cybersecurity within the business processes.

Information management, being an essential part of good IT governance, is a cornerstone at Infosys and has helped provide the organization with a robust foundation. Care is taken to ensure that standardized policies or guidelines apply to and are practical for the organization's culture, business, and operational practices. Cybersecurity requires participation from all spheres of the organization. Senior management, information security practitioners, IT professionals, and users have a pivotal role to play in securing the assets of an organization. The success of cybersecurity can only be achieved by full cooperation at all levels of an organization, both inside and outside and this is what defines the level of commitment here at Infosys.

As a final level of defense, we undergo many internal audits as well as external attestations and audits in a year at an organization level (e.g. SSAE-18 SOC 1 & SOC 2 Type II, ISO 27001). We also undergo client account audits to assess our security posture and compliance against our obligations on an ongoing basis.

There was no material cybersecurity incident reported in fiscal 2025.

Our industry contributions and thought leadership

In this era of rapid technology disruptions and digital transformations, Infosys enables the businesses to embrace innovations and adapt to new technologies. We focus on strengthening cyber resiliency through platform led convergence and consolidation of security capabilities and deliver AI-first service offerings.

We promote cybersecurity through various social media channels such as LinkedIn, Twitter, and YouTube; sharing our point of views, whitepapers, service offerings, articles written by our leaders, their interviews stating various perspectives, and podcasts through our corporate handles providing cybersecurity thought leadership. The topics include impact of evolving technologies such as GenAI on cybersecurity, cloud security, data privacy and protection, and compliance, etc. In addition to this, we work with analysts such as PAC Group and industry bodies such as Data Security Council of India (DSCI), Information Security Forum (ISF), etc. to create joint thought leadership that is relevant to the industry practitioners. In our efforts to strengthen cyber awareness across social communities, we also participate in cybersecurity awareness initiatives led by non-profit organizations such as NASSCOM. Further, we publish a technology centric report that provides insights into emerging technology trends and how they can be applied to businesses. It essentially acts as a guide for enterprises looking to navigate the evolving digital landscape and make informed technology decisions based on current trends. We also host various global chapters of Infosys regularly that aim to be a catalyst for innovation and transformation in the cybersecurity domain. The distinguished members of the council collaborate to discuss, strategize, and prepare roadmaps to address the current security challenges of member organizations and help decipher the evolving industry trends. We, therefore, through various channels, drive awareness of and appreciation for cybersecurity.

Vulnerability Management

The vulnerability management program at Infosys follows best-in-class industry practices coupled with top-notch processes that have been evolving over the years. Rich experience of deftly managing the end-to-end vulnerability life cycle of Infosys Network and the constant hunger to stay abreast of the latest tools, technologies and related market intelligence have acted as a catalyst in fortifying the overall vulnerability management program.

A robust enterprise vulnerability management program builds the foundation for healthy security hygiene of an organization. The following practices have been put in place at Infosys for,

1. Real time asset discovery followed by instantaneous identification of vulnerabilities, misconfigurations, and timely remediation
2. Automation of vulnerability management, configuration compliance, security assessments and review for assets, applications, network devices, data, and other entities in real time
3. Close coupling of detection and remediation processes; auto prioritization to reduce the turnaround time for closure of detected vulnerabilities
4. Continuous monitoring of all public facing Infosys sites and assets for immediate detection of vulnerabilities, ports, or services
5. Regular penetration testing assessments and production application testing for detection and remediation of vulnerabilities on a real time basis