Information management

Infosys Cybersecurity is an amalgamation of the strategy that supports our cybersecurity framework - SEED - and a strong cyber governance program driven through the Information Security Council.

The strategy is designed to minimize cybersecurity risks and align to our business goals. It focuses on proactive enablement of business, besides ensuring continual improvement in the compliance posture through effective monitoring and management of cyber events. We believe that an effective security culture would complement our cybersecurity objectives by reducing enterprise risks. The Infosys Cybersecurity Program ensures that required controls and processes are implemented, monitored, measured, and improved continuously to mitigate cyber risks across domains.

Infosys is committed to:

- Protect the confidentiality, availability, and integrity of information assets from internal and external threats.
- Ensure and maintain stakeholders trust and confidence about cybersecurity.

The executive cybersecurity governing body is in place to direct and steer:

- Alignment of cybersecurity strategy and policy with business and IT strategy.
- Value delivery to stakeholders.
- Assurance that cyber risks are being adequately addressed.

Approach

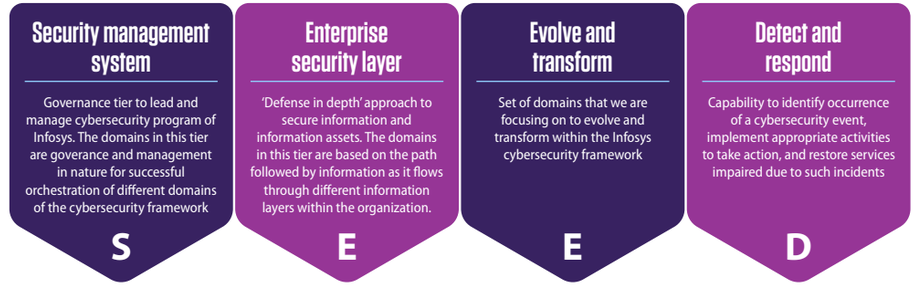
WHAT	SECURE BY DESIGN	SECURE BY SCALE	SECURE THE FUTURE
WHY	• Maximize visibility • Minimize risk • Early engagement	• Optimize cost • Amplify reach • Rapid development	• Innovate faster • Deliver value • Thought leadership
HOW	• Awareness and culture • Security architecture • DevSecOps • Intuitive dashboards • Compliance	• Platforms and accelerators • Integrated and optimized • Automation • Managed security service • Academic collaboration	• Competency building • Research and innovation • Co-created partner solution • Emerging technologies

Cybersecurity strategy and governance

The high-level objectives of the cybersecurity program at Infosys are:

1. Proactive business security and employee experience
2. Continuously improve security posture and compliance
3. Effective management of cyber events and
4. Building a security culture

The Infosys' cybersecurity framework - SEED - is built based on leading global security standards and frameworks such as the National Institute of Standards Technology (NIST) cybersecurity framework and ISO 27001, and is structured around these areas:



The framework also entails a comprehensive cybersecurity maturity model, which helps to ascertain the cybersecurity maturity as well as benchmark against industry peers on an ongoing basis.

This helps in continued oversight and commitment from the Board and senior management through the Information Security Council (ISC) and the Cybersecurity sub-committee.

In keeping with the 'defense in depth' philosophy, we have deployed several layers of controls to ensure that we keep our and our client data secure.

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 with 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. There is a concerted effort from the top management to our end users in the development and implementation process. Additionally, 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 (e.g.: SSAE-18, ISO 27001) as well as client account audits to assess our security posture and compliance against our obligations on an ongoing basis.

There was one substantiated cybersecurity incident reported in fiscal 2024.

Our industry contributions and thought leadership

Infosys promotes cybersecurity through various social media channels such as LinkedIn, Twitter, and YouTube, sharing our point of views, whitepapers, service offerings, articles written by leaders, their interviews, and podcasts through our corporate handles providing thought leadership. In addition to this, we work with analysts such as PAC Group and industry bodies such as Data Security Council of India, Information Security Forum etc. to create joint thought leadership that is relevant to the industry practitioners. Our niche report "Invisible tech, Real impact.", based on a study done in partnership with Interbrand (a top brand consultancy firm) estimates the impact on brand value due to data breaches. We also host various global chapters of the Infosys CISO advisory council regularly that aims 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.

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. The rich experience of deftly managing end-to-end vulnerability life cycle of the 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.

The vulnerability remediation strategy of Infosys focuses on threat-based prioritization, vulnerability ageing analysis and continuous tracking for timely closure. We have successfully eliminated the ticketing system for vulnerability tracking by establishing a continuous detection and remediation cycle, where the IT teams are enabled and onboarded onto the vulnerability management platform. A cybersecurity awareness culture is nurtured, and teams are encouraged to proactively remediate the vulnerabilities reported on their assets or applications.

Supply risk management

A comprehensive supplier security risk management program at Infosys ensures effective management of potential security risks across the various stages of supplier engagement. The process comprises:

- Categorization of the suppliers based on the nature of the services provided and the sensitivity of the data involved.
- Defining standardized set of information security controls as applicable to each category of supplier.
- Defining, maintaining, and amending relevant security clauses in the supplier contracts as applicable to each category of supplier.
- Due diligence, security risk assessment for effective management of the information security risks associated with suppliers.

Defining and monitoring of key security metrics for suppliers (e.g., background check, security awareness training completion, timely interventions regarding information security incidents etc.) threat intel tracking, and governance further strengthen the Infosys supplier security risk management program.

Cybersecurity skill management

With the increasing demand for cybersecurity jobs and a skilled workforce, Infosys has taken several measures to counter the cybersecurity talent crisis and skill, retain and diversify its security workforce in areas such as application security and secure development lifecycle.

Cybersecurity team members undergo technical as well as behavioral trainings on an ongoing basis. Infosys internal training programs, as well as external bodies with cybersecurity subject matter expertise, are leveraged for the same with a strong focus on learning through the classroom as well as on-the-job trainings.

- Over 4,400 professionals underwent Purdue training on cybersecurity.
- Infosys utilizes its partnership with NIIT to have its professionals undergo a Cybersecurity Master's Program.

Building, strengthening, and upholding a positive and sustainable cybersecurity culture

At Infosys, driving a positive and sustainable cybersecurity culture is one of the key constituents of our robust cybersecurity strategy. While we embrace top-notch tools and technology to bulk up our cybersecurity stance, the 'human factor' is equally an area of sharp focus for us. Various measures are in place to nurture a confident and empowered cybersecurity mindset, and we believe in democratizing security in its truest sense. We have embraced the Secure by Design (SbD) approach at an organizational level and offer multiple trainings / drive awareness on SecureSDLC, as part of this initiative. Diverse and proactive communication campaigns are driven across the organization by leveraging various awareness means / tools, including posters, advisories, emails, push messages, mandatory awareness quizzes, gamification, SME Cyber Talks, awareness sessions, videos, podcasts, fireside chats, panel discussions, focused social engineering awareness, security courses on the internal learning platform, thought leadership messages, surveys, annual cybersecurity week celebration etc. There is also an interactive 3D animated e-learning certification program that helps drive positive security behavior amongst the Infoscions.

Innovations for our clients

Infosys innovation-led offerings and capabilities

- Cyber Next platform-powered services help customers stay ahead of threat actors and proactively protect them from security risks. Our pre-engineered packaged and managed security services help monitor, detract, and respond by getting extensive visibility and actionable insight through threat intelligence and threat hunting. Our offerings ensure risk-based vulnerability management by providing a comprehensive single pane of glass posture view. We have made huge progress in the Cyber Next platform-powered service delivery through various modules - Cyber Watch, Cyber Intel, Cyber Hunt, Cyber Scan, Cyber Gaze, Cyber Compass, Cyber Central that ensure comprehensive Managed Protection Detection and Response (MPDR) for our global customers.
- Zero Trust Security architecture and solutions to navigate our customers to embrace zero trust security. Key innovation and offerings include Secure Access Service Edge (SASE) delivered as-a service. With SASE as-a Service, we ensure strengthened overall security through cloud delivered security controls and capabilities. Infosys innovation in policy standardization enforce controls ataccess level, accelerate rollout of service thereby reducing or eliminating legacy tools allowing our customers to reduce overall costs while enhancing end-user experience.
- Secure Cloud transformation with Cobalt assets drive accelerated cloud adoption. With Secure Cloud reference architecture and Secure by Design principle we ensure security is embedded as part of cloud strategy, design, implementation, operations, and automation.

Industry recognition

- **Analyst recognition:**
  Positioned as a Leader- U.S, in "CyberSecurity - Solutions & Services 2021 ISG Provider Lens™ Study"
- **Client testimonies:**
  Infosys CyberSecurity services was recognized by two of our esteemed clients bpost and Equatex
- **Cummins and Infosys:**
  Securing Identities Together
- **Client testimonies:**
  Infosys provides Managed Protection, Detection and Response to bpost (Belgian Post Group)
- **Client testimonies:**
  Infosys secures MS Amlin's digital transformation journey
- **Analyst Testimonial:**
  Infosys is among the world's leading providers of Managed Security Services (MSS), says Frank Heuer, Cybersecurity Analyst at Information Services Group (ISG)
- **Analyst Rating:**
  Infosys positioned as a Leader in the ISG Provider Lens™ Cybersecurity – Solutions and Services 2023 for U.S.
- **Analyst Rating:**
  Infosys positioned as a Leader in the ISG Provider Lens™ Cybersecurity – Solutions and Services 2023 for Europe.
- **Analyst recognition:**
  Infosys CISO crowned as "The Cyber Express Cybersecurity Persons of 2023(India)"