NCR ATLEOS

CXO strategic report 2025

Cybersecurity challenges in future enterprise connectivity

ncratleos.com

Executive summary

As enterprise networks expand and integrate AI and IoT technologies at scale, cybersecurity has moved from being a technical function to a boardroom concern. This report is a CXO-level synthesis of insights from an AT&T Enterprise Leadership Forum workshop held in Bangalore, India. It addresses the multi-layered security challenges brought on by decentralized infrastructure, shadow AI, policy inconsistency and the erosion of traditional trust boundaries.

The findings emphasize a forward-thinking cybersecurity posture—one that is policy-driven, decentralized and deeply embedded into business strategy.

The cybersecurity landscape: critical challenges

IoT endpoint explosion and systemic risk

Enterprises are deploying millions of IoT endpoints—sensors, cameras, wearables and smart appliances—across supply chains, plants, retail spaces and offices. Most of these devices lack inherent security controls due to limited processing capacity, are often not updated regularly and may run outdated firmware. These endpoints form an attack surface that is nearly impossible to secure through traditional antivirus or endpoint protection methods. A single insecure device can act as a gateway to critical enterprise systems. Without micro-segmentation or localized security, enterprises risk lateral movement by threat actors once one device is breached.

Decentralized work models vs. policy enforcement

The shift to hybrid and remote work has led to the increased use of mobile devices and employee-owned hardware. Cybersecurity policies often lag behind real-world use. Employees require access to enterprise systems from mobile apps and personal networks, but this convenience weakens visibility and control. Inconsistent policy enforcement results in fragmented security postures, with some endpoints fully protected and others highly vulnerable.

Rise of unregulated and shadow AI use

Teams across functions—from engineering to marketing—are experimenting with generative AI tools like ChatGPT, Copilot and open-source LLMs. Many of these tools are used without formal IT approval or monitoring, leading to the uncontrolled transfer of sensitive corporate data to third-party platforms. Enterprises lack visibility into how AI is being used, where data is being sent and whether any compliance frameworks are being breached. Sensitive data such as source code, customer PII or financial models may be inadvertently shared with external AI systems, resulting in regulatory, reputational or IP-related damage.

Strategic imperatives for enterprise security

Localized security and edge segmentation

Move away from centralized, perimeter-based security. Push controls to the edge—closer to the device and data layer. Deploy micro-networking or segmentation at the facility/site level. Create isolation zones for vulnerable devices and limit lateral movement through ingress and egress filtering. This approach contains breaches and ensures that compromise in one area doesn't cascade across the network.

Enterprise AI governance models

Establish a formal governance framework for AI adoption. This includes role-based access to enterprise-approved AI tools, data anonymization layers and centralized logging of AI interactions. Develop a secure internal 'AI sandbox' where teams can experiment safely. This enables innovation while protecting sensitive data.

Harmonized security policies across platforms

Traditional security policies are often rigid and binary. Adaptive, context-aware policies are needed in modern environments. Use factors like geo-location and device reputation to dynamically allow or restrict access. This balance supports productivity without compromising security.

Zero Trust architecture as a foundational principle

Adopt a Zero Trust approach—trust no device, user or system by default. Use continuous validation for access, encrypt all internal communications and regularly audit privileges. This prevents lateral movement and restricts unauthorized access, even post-breach.

Secure edge infrastructure and endpoint hardening

Standardize baseline security for all deployed hardware, including low-power edge devices. Pre-validate for secure boot, encrypted firmware and lightweight security agents. Require compliance from vendors and integrate monitoring from day one.

Embedding cybersecurity culture across the enterprise

Cybersecurity must be a shared responsibility. Educate teams on AI risks, phishing and best practices. Tie cyber-hygiene to performance reviews and empower business units to take ownership. CXOs should sponsor cross-functional security programs to build resilience into the organizational culture.

CXO recommendations at a glance

Focus area	Strategic action
Governance	Establish AI oversight committees and update acceptable use policies.
Policy enforcement	Move toward adaptive, dynamic security policies.
IT infrastructure	Mandate segmentation and localized controls for edge/IoT zones.
Talent and training	Make security literacy part of workforce development.
Tooling	Invest in AI-safe environments, Zero Trust platforms and secure mobile work solutions.
Third-party risk	Audit and enforce security requirements for all device and platform vendors.

AT&T capabilities

Helping guard its network and customers against threats is in AT&T's DNA. From the telegraph to 5G, it matches technology progress with security innovation. AT&T operates one of the world's most advanced and powerful global backbone networks. It has hundreds of cybersecurity experts—some of the most savvy and sophisticated in the world. They help protect more than 465 petabytes of data flowing across its network daily. They develop and use tools including automation, algorithms, AI and shared alerts. It's all in the service of more securely connecting customers to what matters most in their daily lives.

NCR Atleos capabilities

NCR Atleos partners with the leading communications service providers and systems integrators to help them expand their portfolio and extend their global reach.

NCR Atleos' broad services portfolio and extensive multivendor expertise keep physical, virtual and cloud-based networks running at peak performance.

Design, deploy, maintain: NCR Atleos ecosystems bring together the best-in-class hardware, software and services to deliver on what customers want, when they want it.

Conclusion: Leading the digital future securely

The convergence of AI and IoT is unlocking massive business value—but it's also redrawing the boundaries of enterprise risk. For CXOs, cybersecurity is no longer a reactive IT function; it is a strategic pillar of trust, compliance and business continuity.

By embedding security into architecture, operations and culture, forward-looking organizations can embrace innovation without compromise. The future belongs to those who can govern flexibly, move decisively and secure deeply.

About this report

This document was developed based on insights from the roundtable, "Cybersecurity challenges in future enterprise connectivity," at the AT&T Enterprise Leadership Forum. This report summarizes the discussion and perspectives shared during the roundtable. The views expressed are those of the individual participants and do not represent the official position of AT&T or NCR Atleos.

Source: Source: AT&T Enterprise Leadership Forum workshop. In partnership with NCR Atleos.

Contact us at NCRAtleos.com today

About NCR Atleos

NCR Atleos (NYSE: NATL) is a leader in expanding self-service financial access, with industry-leading ATM expertise and experience, unrivalled operational scale including the largest independently-owned ATM network, always-on global services and constant innovation. NCR Atleos improves operational efficiency for financial institutions, drives footfall for retailers and enables digital-first financial self-service experiences for consumers. NCR Atleos was ranked #12 in Newsweek's prestigious 2025 Top 100 Global Most Loved Workplaces® list. NCR Atleos is headquartered in Atlanta, Ga., with approximately 20,000 employees globally. For more information, visit www.ncratleos.com.

NCR ATLEOS

NCR Atleos continually improves products as new technologies and components become available. NCR Atleos, therefore, reserves the right to change specifications without prior notice.

All features, functions and operations described herein may not be marketed by NCR Atleos in all parts of the world. Consult your NCR Atleos representative or NCR Atleos office for the latest information.

NCR Atleos is either a registered trademark or trademark of NCR Corporation in the United States and/or other countries. All brand and product names appearing in this document are trademarks, registered trademarks or service marks of their respective holders.