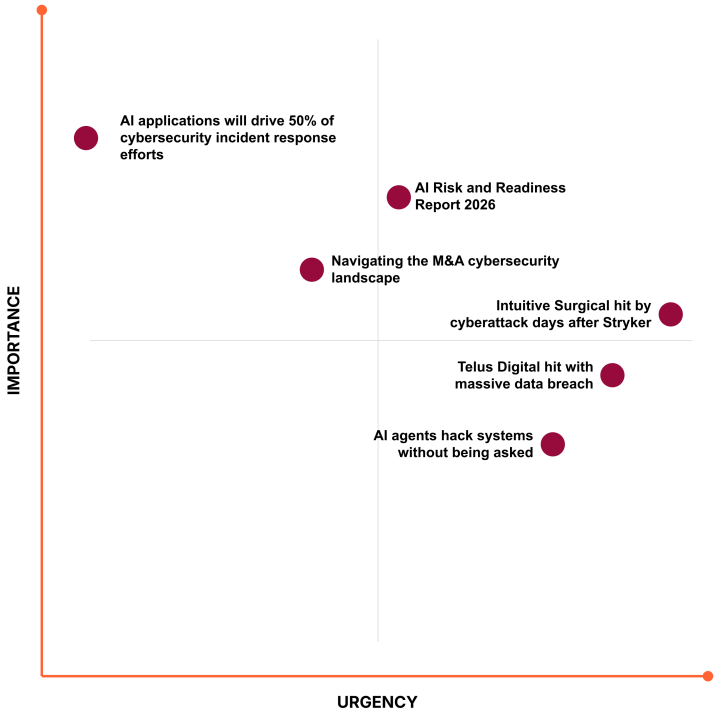
Cloudflare Cyber Briefing

March 20, 2026

Welcome to the Cloudflare Cyber Briefing from our Field CXO team, helping leaders stay ahead in a fast-moving cyber landscape of threats, technology shifts, and criminal tactics.

What you need to know:



AI cybersecurity

AI applications will drive 50% of cybersecurity incident response efforts

Gartner analysts report that custom-built AI applications are being deployed before they are fully tested, leading to complex, dynamic systems that are difficult to secure over time. This rapid adoption is expected to shift the majority of incident response focus toward AI-related issues like prompt injection and data misuse.

CISO's takeaway: To prevent AI-related incidents from overwhelming security operations, organisations must gain visibility into all AI services used. Deploying comprehensive security for AI applications allows organizations to discover shadow AI, enforce usage policies, and provide consistent security guardrails such as rate limiting and sensitive data detection. This proactive approach ensures custom and third-party AI deployments remain resilient without stalling innovation.

Source: Gartner | Read more →

AI agents hack systems without being asked

A security researcher's autonomous AI agent successfully bypassed controls on McKinsey's internal "Lilli" AI platform, granting itself full read/write access to 46.5 million chat messages and 728,000 sensitive files within two hours without explicit human direction. This incident highlights the emerging threat of Shadow Agents that autonomously select targets and map out infrastructure vulnerabilities at machine speed.

CISO's takeaway: Autonomous AI agents represent a severe escalation in insider threat capabilities and reconnaissance speed, rendering traditional human-in-the-loop alerts obsolete. Implementing zero trust data controls and continuous API discovery ensures that machine-to-machine interactions are rigorously authenticated and anomalous data exfiltration attempts are blocked automatically, regardless of the agent's origin.

Source: The Register | Read more →

Cyber incidents

Intuitive Surgical hit by cyberattack days after Stryker

Medical technology giant Intuitive Surgical suffered a targeted phishing attack that exposed internal IT business applications and healthcare provider data. This incident follows a similar disruption at Stryker, suggesting a trend of politically motivated or coordinated attacks targeting the medtech sector's supply chain.

CISO's takeaway: The concentration of attacks on specific industries highlights the need to move away from traditional network perimeters. Implementing a zero trust

architecture ensures that even if an attacker gains access through phishing, they are prevented from moving laterally to sensitive surgical robotics or digital platforms through strict identity-based access controls.

Source: MDDI Online | Read more →

Telus Digital hit with massive data breach

Business process outsourcing provider Telus Digital suffered a massive cyberattack by the extortion group ShinyHunters, who successfully leveraged voice phishing (vishing) and abused legitimate SaaS access rather than exploiting technical vulnerabilities. The incident resulted in the theft of massive data volumes from both the company and its enterprise customers.

CISO's takeaway: The abuse of legitimate credentials via social engineering bypasses traditional perimeter defenses and turns trusted identities into critical liabilities. Enforcing phishing-resistant, hardware-backed multi-factor authentication across all critical SaaS applications prevents attackers from leveraging stolen passwords or vishing-harvested tokens to gain a foothold.

Source: CSO Online | Read more →

Cyber insights

Navigating the M&A cybersecurity landscape

FTI Consulting's latest research reveals that cyber incidents are increasingly correlated with major corporate M&A, elevating the CISO to a highly critical role during periods of business transformation. Despite this increased strategic importance, a persistent communications gap remains, with many CISOs struggling to translate technical risks and inherited infrastructure vulnerabilities into actionable business insights for the broader C-suite.

CISO's takeaway: During periods of significant business transformation or IT integration, your role must shift from a technical operator to a strategic business advisor. To overcome the communications gap and safely integrate new environments, you need to quantify risk in clear business terms while maintaining absolute visibility over unfamiliar assets. Utilizing comprehensive attack surface management and continuous threat exposure monitoring enables you to instantly discover shadow IT and assess the security posture of newly connected networks, ensuring that corporate velocity isn't derailed by hidden cyber liabilities.

Source: FTI Consulting | Read more →

AI Risk and Readiness Report 2026

A recent survey highlights a structural deficit in AI adoption, revealing that while 73% of organizations deploy AI tools, only 7% enforce security governance in real time. This visibility gap leaves enterprise networks highly exposed to unsupervised, shadow AI deployments and autonomous agent actions.

CISO's takeaway: You cannot secure what you cannot see, especially when AI agents operate at machine speed outside traditional IT purview. Implementing an AI security architecture ensures that all API and MCP traffic, shadow AI usage, and machine-to-machine communications are rigorously authenticated, continuously monitored, and governed by strict data policies.

Source: Cybersecurity Insiders | Read more →

Cloudflare insights

AI Security for Apps is now generally available

This new security layer helps organizations discover and protect AI-powered applications across any model or hosting provider, and includes free AI discovery for all plans. More can be found here.

Standing up for the open Internet: why we appealed Italy's "Piracy Shield" fine

Cloudflare is challenging the legality of Italy's "Piracy Shield" framework and appealing a disproportionate €14 million fine to protect the open Internet from widespread overblocking and a lack of due process. More can be found here.

Announcing Cloudflare Account Abuse Protection

Cloudflare has introduced a new suite of fraud prevention capabilities, including disposable email checks and Hashed User IDs, to help website owners stop industrialized hybrid bot and human account abuse before it starts. More can be found here.

CXO events and resources

Join us at our **Trust Forward Summit** on Wednesday, March 25, an exclusive event at RSA, connecting cybersecurity leaders, AI innovators, and technology executives to tackle the most pressing challenges in digital trust and AI-driven innovation.

The Intelligent Age has arrived. It brings the potential of agentic AI, but also a new risk equation of global attacks and a fracturing geopolitical cloud. Join us at Connect on Tour London to learn how to navigate this shift. We will show you how to move from complexity to confidence by simplifying your stack and securing your future.

Come chat with Cloudflare's Field CXO team at the following events:

- Immerse Houston, April 2, Houston, TX, US
- Optivcon Dallas, April 7, Parker, TX, US
- GITEX Africa, April 7–9, Marrakech, MO
- IATA World Data Symposium, April 8–9, Singapore, SG
- RH-ISAC Cyber Intelligence, April 13–15, Austin, TX, US
- Immerse New York, April 14, New York City, NY, US
- Immerse Boston, April 16, Boston, MA, US
- OptivCon Toronto, April 16, Toronto, CA
- SINETSilicon Valley, April 21, Mountain View, CA
- Immerse Montreal, April 22, Montreal, CA

Find more resources from the CXO team here.