CYBERSECURITY TRENDS FOR 2026

1 AI-DRIVEN ATTACKS BECOME STANDARD

Attackers use AI to create convincing phishing, automate scanning, and find vulnerabilities faster.

IDENTITY BECOMES THE PRIMARY BATTLEGROUND 2

Stolen credentials cause most breaches.
MFA fatigue and session hijacking rise sharply.

3 CLOUD MISCONFIGURATIONS REMAIN THE TOP RISK

Simple mistakes. Huge consequences.
Companies continue to struggle with cloud complexity.

RANSOMWARE SHIFTS TO PURE DATA EXTORTION 4

Attackers no longer rely on encryption.
They steal sensitive data and threaten to publish it.

5 OT AND CRITICAL INFRASTRUCTURE ATTACKS INCREASE

Hospitals, energy grids, and manufacturing systems become prime targets because they can't afford downtime.

CYBER-RESILIENCE BECOMES ESSENTIAL 6

Companies focus less on avoiding attacks and more on bouncing back quickly.

7 DEEPFAKE FRAUD GROWS RAPIDLY

Fake voices and videos become cheap tools for social engineering and financial scams.

REGULATORY PRESSURE GETS STRONGER 8

Governments tighten cybersecurity rules.
Companies must prove cyber maturity, not just claim it.

9 SUPPLY CHAIN ATTACKS KEEP EXPANDING

Hackers target small vendors to gain access to larger, better-protected organizations.

SKILLS SHORTAGES RESHAPE HIRING 10

Companies hire based on ability, not degrees.
Upskilling accelerates.