State of Cybersecurity in 2026

February 12, 2026

NCTECH Association

A look back — what 2025 taught us

859,532 IC3 internet crime complaints (latest annual report year)

$16.6B IC3 reported victim loses (+33% YoY Increase)

193,407 IC3 phishing/ spoofing complaints (top category)

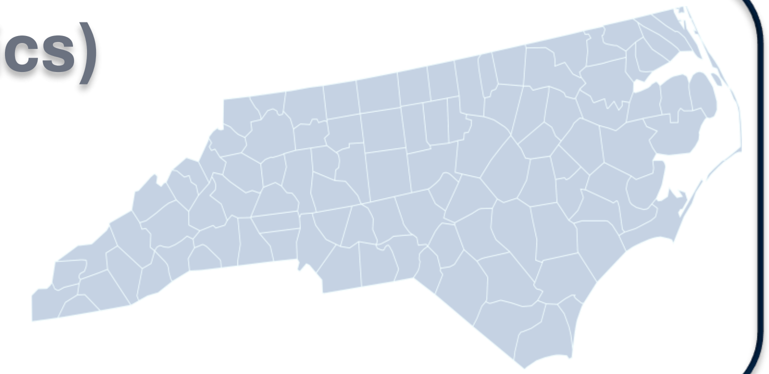
44% Breaches involving ransomware.

88% SMB breaches involving ransomware.

64% Ransomware victims that did not pay. (Median ransom paid $115,000)

North Carolina snapshot (IC3 overall state statistics)

- 22,021 complaints (Ranked in Top 10)
- $324.3M reported losses
- Latest annual report year (2024)



Cybersecurity in 2026 is a speed-and-scale problem:

Threat Actors are moving faster than human-led processes

Threat actors have industrialized access (stolen credentials, malware-free tradecraft, access brokers).

AI increases persuasion and throughput (better phishing, voice fraud/vishing, faster recon).

Vulnerability exploitation is accelerating; especially on edge devices and cloud control planes.

The defender constraint is people: a persistent skills gap and operational coverage limits

What we will see in 2026

AI Driven Cyber Attacks

- Advanced Deepfake Attacks
- Self Learning Malware and AI enabled Evasion
- Automated Vulnerability Scanning & Exploitation
- AI-Powered Distributed Denial of Service Attacks

Geopolitical Tensions

- State Sponsored Attacks
- Hactivism and Protests
- Supply Chain Vulnerabilities
- Increased Regulatory Pressure

Supply Chain Interdependencies

- Third Party Vendor Breaches – Payment Processing, Cloud Storage, accounting and SaaS providers
- Lack of Vendor Management, 3rd Party Risk Assessment or Security Standards

Cyber Skills Gap

- Digital Transformation and IT complexity
- Cybersecurity Education & Training Programs
- Burnout and High Turnover Rates
- Global Competition for Cybersecurity Talent

Deepfake-driven Fraud

- Deepfakes turn “trust” into an attack surface
- The capability is scaling fast and getting cheaper
- “Verification debt” becomes a real operational problem

Regulatory Requirements

- Increased Compliance Costs
- Impact on Innovation and Business Agility
- Heightened Risk of Non-Compliance Penalties
- Integration of Privacy & Security Controls

Identity: The New Primary Control Plane

- Cloud + SaaS moved the front door
- Whoever controls logins, tokens, and access policies controls the environment.
- Privileged identities are the highest-value targets

Continuous Threat & Exposure Management

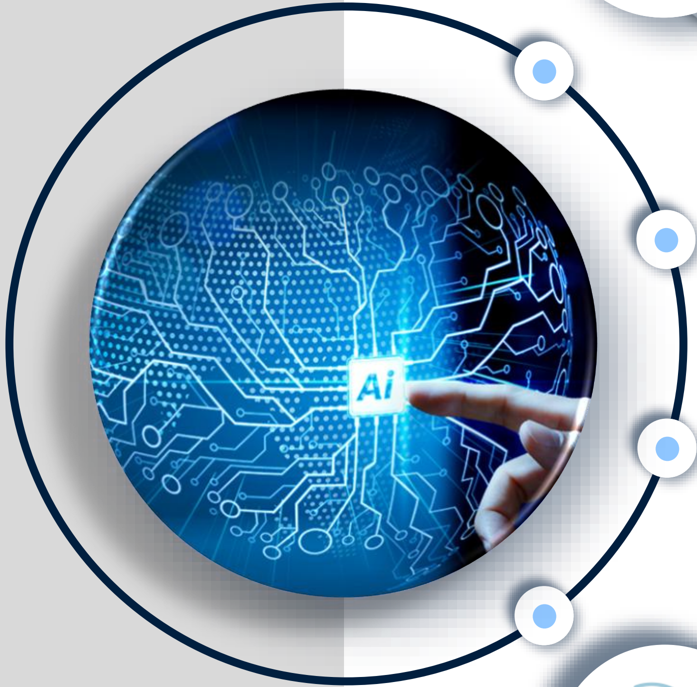
- Shifts risk from “how many vulns” to “which exposures are exploitable right now
- Turns exposure into an operating metric
- Keeps pace with faster exploitation by continuously prioritizing what to fix first

Post Quantum Security Planning

- “Harvest now, decrypt later” turns quantum into a current risk
- The standards race is over; the migration race started
- Government timelines will drive compliance pressure

AI Driven Cyber Attacks

AI doesn’t just create new attacks — it industrializes the old ones: better lures, faster execution, and more ways for sensitive data to leak.



Proliferation: 75% of global knowledge workers reported using GenAI at work. 27% of White-Collar employees state that they “Frequently” use AI at work – Often outside of approved guardrails

Persuasion: AI makes phishing/BEC and deepfake vishing dramatically more convincing. 680% YoY rise in deepfake activity and 475% increase in synthetic voice fraud

Brand-New Attack Surface: Agentic tools (Clawbots/Moltbots/OpenClaw) put “autonomous execution” on endpoints.

Speed + Sophistication: AI helps criminals and APTs move faster through the kill chain

Geopolitical Tensions

Geopolitical conflict is a cyber force-multiplier and turns SMBs into Collateral damage.

More Hands on Keyboards: Hacktivist-driven activity dominates incident reporting (~80% of recorded incidents) .

DDoS & outages become strategic messaging: While phishing remains the dominant intrusion vector (60%), disruption activity remains heavily represented in the same landscape

Your risk = your dependencies: 54% of mid-market organizations cite supply-chain interdependencies as the biggest barrier to cyber resilience (Vendors, SaaS, MSPs)

Instability keeps extortion profitable: ~$813.6M in ransomware payments in 2025 and notes ransomware groups increasingly focus on small-to-mid markets.

Supply Chain Interdependencies

In 2026, attackers don't breach you—they breach your supply chain.

Their Incident – Your Risk: third-party involvement in breaches doubled from 15% to 30%

High ROI Target: Supply-chain compromise is one of the most common AND one of the most expensive breach entry points

Larger Blast Radius: A single exploited vulnerability or flaw in products used by MSPs/SaaS/Edge Devices can cascade into hundreds or thousands of mid-market environments.

Threat Surface Expansion: Supply Chain is expanding into "agentic" and AI-enabled services—meaning more integrations, more tokens, more third-party access paths, and more chances to misconfigure trust.

Cyber Skills and Resource Gap

If you can't staff defense, attackers won't just breach you, they'll run your business for you.

You Can't Hire what doesn't exist: ~4.8M global cybersecurity workforce gap (ISC2)

Skills gaps are widespread and worsening: 66% report moderate-to-critical skills gaps; only 14% feel adequately staffed

Skills gap = measurable breach cost increase: +$1.76M average breach cost impact tied to skills shortages

Ransomware pressure is concentrated in SMBs: Ransomware/extortion malware in 88% of SMB breaches

Identity: The New Primary Control Plane

Identity is the new perimeter: if attackers control accounts, tokens, or MFA, they control what your business can access.

Attackers prefer “log in” over “break in”: stolen creds, tokens, and session hijacks bypass many traditional defenses.

Cloud/SaaS made identity the front door: access to M365, finance apps, and data is governed by IdP policies (not the firewall).

Privilege is the blast radius: one admin takeover can create accounts, change MFA, grant OAuth consent, and exfiltrate data “legitimately.”

Control-plane posture = your real security posture: phishing-resistant MFA, conditional access, PAM/JIT, and OAuth/token governance are now top-tier controls.

Continuous Threat & Exposure Management

If you can’t staff defense, attackers won’t just breach you, they’ll run your business for you.

MITIGATE
ASSESS
MONITOR
IDENTIFY
REVIEW
RISK MANAGEMENT

3× fewer breaches: Gartner says orgs using CTEM to prioritize security investment will be **3x less likely** to suffer a breach by 2026.

Edge exploitation is surging: Verizon notes edge/VPN devices were **22% of exploitation targets**—a CTEM priority zone.

Patch lag creates a window: Only **~54%** of edge device vulns were fully remediated (median **32 days**). CTEM is built to shrink that window.

Prioritize what’s real: CISA KEV focuses teams on vulns **actively exploited in the wild**, not “CVSS noise.

Deepfake Driven Fraud

Deepfakes are turning trust into a vulnerability; attackers can now “be” your CEO, vendor, or customer on demand, and midmarket organization aren’t built to survive that

It scales like software, not like crime: Generative AI is making fraud more believable and easier to execute at scale (AI-generated text, voice, video used for social engineering and financial fraud).

It’s already producing catastrophic corporate losses. A widely reported case involved criminals using deepfake participants on a video call to convince an employee to transfer **over $25M**.

The attempt volume is exploding. A **deepfake attempt occurred every five minutes in 2024**, There is major growth in related digital forgery activity; evidence this is becoming industrialized, not occasional.

It supercharges the midmarket’s #1 fraud channel: payment diversion: BEC as a multi-billion-dollar problem, and industry summaries cite billions in annual losses—deepfake voice/video makes “verify the request” dramatically harder.

Regulatory Pressure

Regulatory pressure is now a cyber risk

The compliance map is exploding: 20 U.S. states now have comprehensive consumer privacy laws

Paperwork competes with real security: 76% of CISOs say fragmented regulations create significant compliance challenges

Your customers' rules become your contract risk: Public companies must disclose material cyber incidents within 4 business days of determining materiality

Security attestation is becoming "table stakes": If you support highly regulated industries, gaps can mean lost bids, delayed awards, or expensive last-minute remediation.

Post Quantum Computing

Quantum makes today’s encryption “expire”: RSA/ECC will eventually be breakable, so confidentiality and digital trust become time-limited.

Harvest-now, decrypt-later: data stolen encrypted today can be decrypted later—long-life data is at risk now.

Standards are here, migration is real: NIST finalized PQC standards (FIPS 203/204/205), so “plan” becomes “execute.”

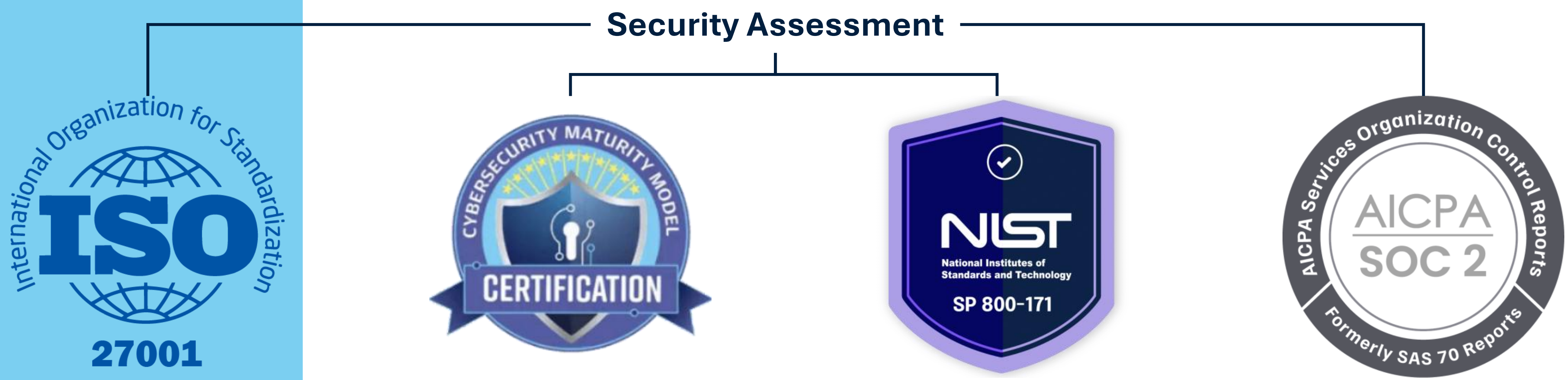
It breaks more than encryption: PKI/certificates, VPN/TLS key exchange, and code/firmware signing all depend on quantum-vulnerable cryptography unless upgraded.

The transition has already started in mainstream protocols: Major platforms are pushing hybrid PQC in HTTPS/TLS and stressing crypto agility to avoid being stuck during the transition..

Define Your Journey

1 Assess Your Current Risk

If you haven’t assessed your security posture against a recognized framework, you’re not managing risk; you’re guessing


Security Assessment

International Organization for Standardization
ISO
27001
CYBERSECURITY MATURITY MODEL
CERTIFICATION
NIST
National Institutes of Standards and Technology
SP 800-171
AICPA Services Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

2

Prioritize Remediation on High Impact Risks

Reduce risk fast by fixing what attackers exploit most—starting with the highest impact, lowest effort controls.

Administrative

Policies, Procedures, Standards, Training, Risk Management

Technical

Security Tools and Configurations (Access Control, Encryption, Endpoint Protection).

Physical

Locks, Badges, Cameras, Secure Facilities, Environmental Protections.

3

Create Awareness

Locks, Badges, Cameras, Secure Facilities, Environmental Protections.

Reinforcement

Your biggest exposure isn’t a zero-day—it’s a trusted user making one bad decision at the wrong moment.

Leadership + Culture

Executives and Managers reinforce expectations, model good behavior, and make it safe to report mistakes

Role-based Continuous Education

Short, frequent training tailored by role and reinforced with real-world simulations.

Measurement + Reinforcement

Track behavior change (simulation results) and follow up with targeted coaching.

4

Adopt a Zero trust Architecture

Assume breach. Trust nothing by default. Verify every access request—every time.

Zero Trust Model
Platform
Data Security

5

Be Vigilant

Security isn’t a project. It’s a measurement discipline: continuously validate exposure, control effectiveness, and attacker activity—before the business pays for it.

Vigilance™
by SilverTree

SilverTree

Thank you

SILVERTREESERVICES.COM

Darwin Herdman

Chief Innovation and Security Officer

Darwin.herdman@silvertreeservices.com

bitly