Colorado Cyber Risk Surface Report

Aggregated Public Cybersecurity Incident Intelligence — May 2026
Prepared for: Client Distribution
Prepared by: Hybraxis Threat Solutions LLC
Date: May 11, 2026

Executive Summary

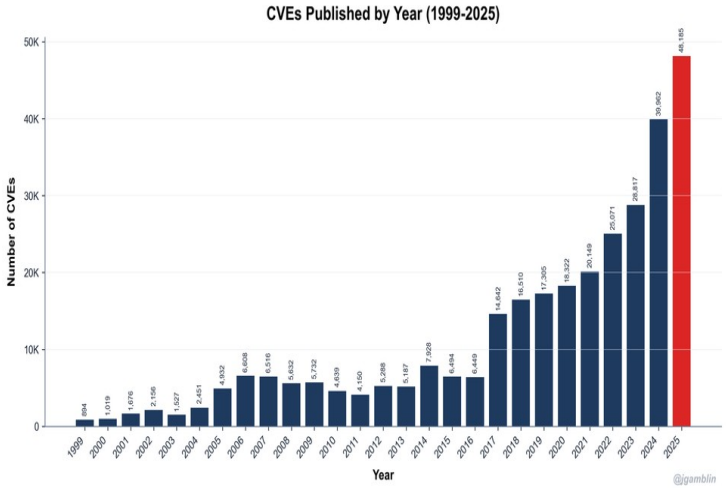
Colorado organizations continue to face a rapidly intensifying cyber threat environment characterized by accelerated vulnerability exploitation, ransomware extortion activity, credential theft, and increasing third-party supply chain exposure. Publicly disclosed cybersecurity incidents throughout the reporting period show a continued concentration of attack activity along Colorado's Front Range economic corridor, particularly within the metropolitan regions of Denver, Colorado Springs, Boulder, Aurora, Fort Collins, and surrounding municipalities.

Healthcare systems, educational institutions, public-sector agencies, and small-to-medium businesses (SMBs) remain disproportionately represented in publicly disclosed breaches. The operational dependence on cloud-hosted services, remote access technologies, identity-based authentication systems, and third-party software ecosystems has significantly expanded the attack surface across both public and private sectors.

Nationally, the cybersecurity landscape continues to worsen due to the unprecedented growth in publicly disclosed software vulnerabilities. According to reporting from MITRE CVE Program and industry tracking organizations, annual CVE disclosures increased from approximately 18,000 vulnerabilities in 2020 to more than 48,000 vulnerabilities disclosed during 2025 alone. This represents a greater than 260% increase in publicly tracked vulnerabilities over a five-year period. Threat actors are increasingly weaponizing newly disclosed vulnerabilities within days — and in some cases hours — of publication, substantially compressing remediation timelines for defenders.

Colorado organizations also continue to face elevated risks associated with:

- Cloud platform compromise
- Identity and access management failures
- Third-party vendor exposure
- Ransomware-as-a-Service (RaaS) operations
- Social engineering campaigns
- Internet-exposed remote management infrastructure
- Weak multi-factor authentication (MFA) implementation
- Legacy operational technology (OT) and healthcare infrastructure



Recent reporting involving compromise activity associated with educational technology ecosystems, including concerns surrounding unauthorized access to cloud-based learning platforms such as Canvas, further demonstrates the increasing prevalence of identity-centric attacks against education and enterprise environments.

While public reporting provides visibility into major incidents, available datasets likely underrepresent the true volume of cyber events impacting Colorado organizations due to inconsistent breach disclosure laws, delayed reporting, reputational concerns, and the prevalence of unreported ransomware extortion incidents.

Colorado Threat Landscape Overview

Geographic Concentration of Incidents

Publicly disclosed incidents continue to cluster heavily along Colorado's Front Range corridor, which contains the state's highest density of:

- Healthcare infrastructure
- Government services
- Defense contractors
- Technology companies
- Financial institutions
- Educational systems
- Critical infrastructure operators

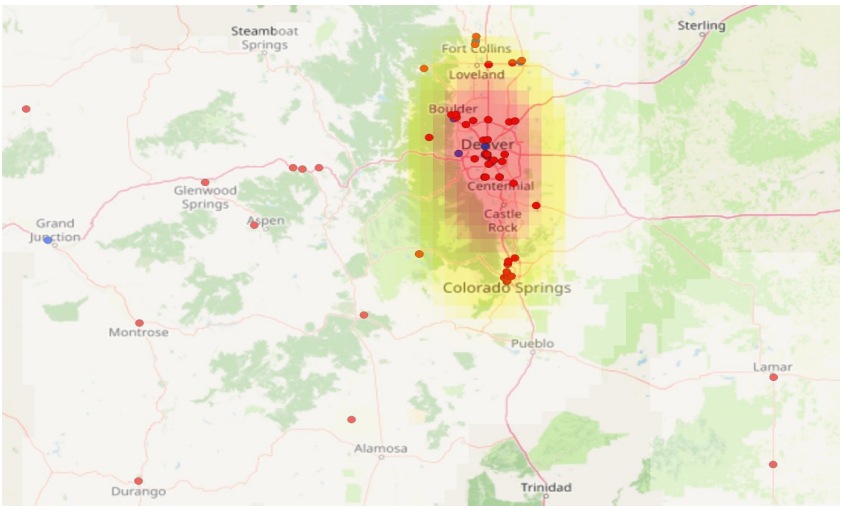


Figure I: Geographic Concentration of only the healthcare industry Cyber Incidents in the Front range from 2020-2026.

(Each plotted incident represents a publicly disclosed breach resulting in the exposure of thousands to tens of thousands of personal records.)

The Denver metropolitan area remains the largest concentration point for reported cyber incidents due to:

- Population density
- Enterprise concentration
- Healthcare system scale
- State government presence
- Cloud and SaaS adoption
- Regional internet infrastructure centralization

Colorado Springs additionally represents a strategically significant cyber target environment due to the concentration of military, aerospace, and defense-sector organizations.

Boulder and Fort Collins continue to demonstrate elevated exposure tied to:

- Research institutions
- Universities
- Biotechnology firms
- High-technology startups
- Distributed cloud infrastructure

Key Findings

Primary Attack Vectors Observed

Ransomware and Network Intrusion

Ransomware operations remain among the most operationally disruptive threats observed during the reporting period. Public disclosures indicate threat actors continue targeting:

- Healthcare providers
- Municipal governments
- K-12 school systems
- Manufacturing organizations
- Legal and financial services firms

Modern ransomware campaigns increasingly involve:

- Double-extortion tactics
- Data theft prior to encryption
- Credential harvesting
- Exploitation of remote management services
- Abuse of unmanaged edge devices
- Supply chain compromise

Common initial access vectors include:

- Phishing emails
- Stolen VPN credentials
- Exploitation of internet-facing appliances
- Remote Desktop Protocol (RDP) exposure
- Vulnerable virtual private network infrastructure

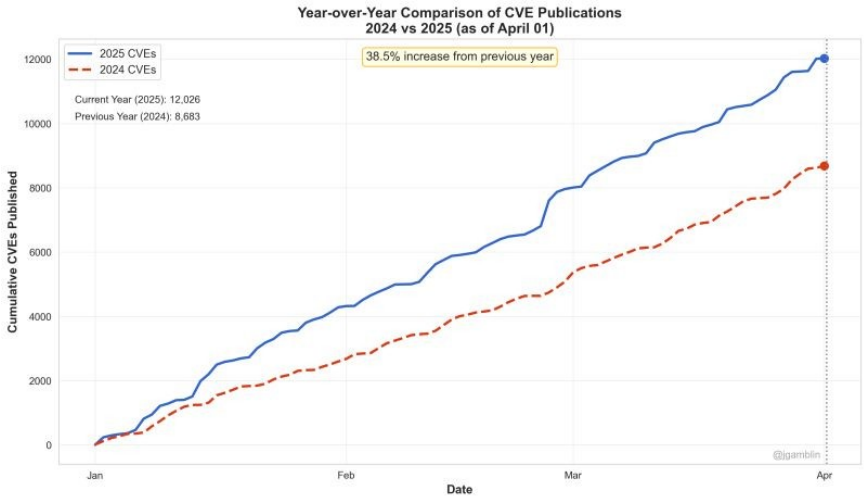


Figure II: CVE Growth 2024-2025

Phishing and Business Email Compromise (BEC)

Phishing remains one of the most persistent and successful attack methods affecting Colorado organizations. Attackers continue leveraging:

- Credential harvesting portals
- MFA fatigue attacks
- Executive impersonation
- Invoice fraud schemes
- Cloud account takeover attempts
- OAuth token abuse

Organizations with hybrid Microsoft 365 and Google Workspace environments remain particularly exposed to identity-based attacks due to:

- Incomplete MFA enforcement
- Weak conditional access policies
- Excessive privilege allocation
- Inadequate monitoring of anomalous login activity

Business Email Compromise continues generating significant financial losses nationally, particularly among SMBs lacking mature email security controls.

Third-Party and Supply Chain Exposure

Third-party compromise risk continues to expand across nearly all sectors. Organizations increasingly rely on:

- SaaS platforms
- Managed service providers (MSPs)
- Cloud identity providers
- Electronic medical record systems
- Payment processors
- Education technology vendors

Single vendor compromise events can expose:

- Sensitive client information
- Authentication systems
- Operational infrastructure
- Backup environments
- Remote administration tools

Recent national cyber incidents continue to demonstrate that vendor ecosystems frequently represent force multipliers for attackers.

Unauthorized Access and Credential Abuse

Credential theft remains a dominant component of modern intrusion activity. Threat actors increasingly leverage:

- Infostealer malware
- Session hijacking
- Password reuse
- Stolen browser tokens
- Dark web credential marketplaces
- Social engineering against help desks and IT support staff

Organizations lacking:

- MFA enforcement
- Identity monitoring
- Privileged access controls
- Endpoint detection

  remain at substantially elevated risk.

Sector Analysis

Healthcare Sector

Healthcare remains one of the most heavily targeted sectors in Colorado and nationally due to:

- High-value patient data
- Operational urgency
- Legacy infrastructure
- Large distributed networks
- Limited downtime tolerance

Threat activity affecting healthcare environments commonly includes:

- Ransomware deployment
- Electronic health record disruption
- Third-party billing exposure
- Credential compromise
- Insider misuse
- Medical device security weaknesses

Healthcare entities also face increased regulatory exposure under:

- HIPAA
- HITECH
- State breach notification laws

Operational disruption within healthcare environments can directly affect patient care continuity, emergency operations, and regional healthcare coordination.

Education Sector

K-12 districts and higher education institutions continue facing elevated attack volumes due to:

- Large user populations
- Decentralized IT administration
- High account turnover
- Bring-your-own-device (BYOD) environments
- Extensive cloud application use

Common attack activity includes:

- Student account compromise
- Ransomware attacks
- Credential stuffing
- Data theft
- Learning platform abuse
- Social engineering campaigns

Educational institutions remain attractive targets due to the volume of personally identifiable information (PII) maintained across students, staff, and faculty systems.

Government and Public Sector

Public-sector organizations continue facing elevated ransomware and phishing threats driven by:

- Legacy systems
- Budget limitations
- Public-facing services
- Critical infrastructure responsibilities

Threat actors frequently target municipalities and agencies due to:

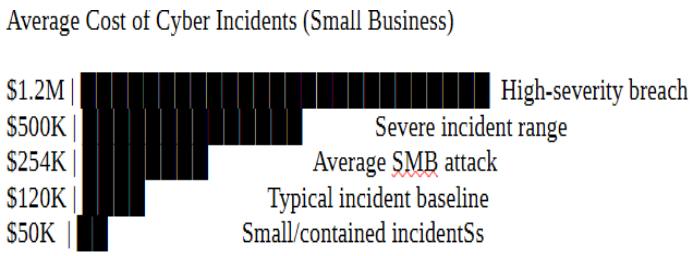
- Operational urgency
- High public visibility
- Sensitive citizen data
- Interconnected vendor ecosystems

Local governments lacking centralized cybersecurity governance remain especially vulnerable to operational disruption.

Small and Medium Businesses (SMBs)

SMBs likely remain substantially underrepresented in public breach reporting despite continued targeting activity. Many smaller organizations:

- Lack dedicated cybersecurity personnel
- Maintain limited monitoring capabilities
- Depend heavily on MSPs
- Operate without mature incident response planning



SMBs increasingly face automated attack activity from:

- Credential stuffing campaigns
- Commodity ransomware operators
- Phishing kits
- Botnet exploitation
- Internet-wide vulnerability scanning

Because many SMB incidents never become publicly disclosed, observed public data likely understates actual regional cyber activity.

Vulnerability and Exploitation Trends

Public vulnerability disclosures continue increasing at record pace.

Industry-wide observations indicate:

- Rapid growth in CVE publication volume
- Increased exploitation of edge devices
- Shortened exploit weaponization timelines
- Growing abuse of zero-day vulnerabilities
- Increased targeting of VPNs, firewalls, and remote access infrastructure

Attackers increasingly prioritize:

- Internet-facing appliances
- Identity infrastructure
- Cloud synchronization tools
- Backup systems
- Remote monitoring and management (RMM) platforms

The average time between vulnerability disclosure and observed exploitation activity has continued shrinking across multiple threat campaigns.

Organizations relying on quarterly or delayed patch cycles may remain operationally exposed long after exploit code becomes publicly available.

Emerging Threat Considerations

AI-Enhanced Social Engineering

Threat actors are increasingly leveraging generative AI tools to improve:

- Phishing quality
- Social engineering realism
- Multi-language campaigns
- Deepfake impersonation
- Automated reconnaissance

This trend may reduce traditional indicators previously used to identify malicious communications.

Cloud and Identity-Centric Attacks

Cyber intrusions increasingly target:

- Single sign-on (SSO) environments
- Cloud identity providers
- OAuth integrations
- API keys and tokens
- Federation trust relationships

Traditional perimeter-based security approaches continue losing effectiveness as organizations migrate infrastructure and workflows to cloud environments.

Critical Infrastructure Exposure

Utilities, transportation systems, healthcare networks, and regional infrastructure providers continue facing heightened risk from:

- State-sponsored activity
- Ransomware operations
- OT/ICS targeting
- Third-party compromise

Colorado’s growing technology and aerospace sectors may continue attracting strategic cyber targeting activity.

Strategic Assessment

Colorado organizations continue operating within a threat environment characterized by:

- Expanding digital attack surfaces
- Increasing vulnerability volume
- Faster exploit weaponization
- Persistent ransomware activity
- Identity-centric attacks
- Third-party dependency risk

Organizations without mature:

- Vulnerability management
- Identity security
- Security monitoring
- Incident response capabilities

- Asset visibility
- Backup validation
- Endpoint detection

remain at elevated operational risk.

Particular concern exists for organizations operating:

- Legacy systems
- Unsupported infrastructure
- Public-facing remote services
- Flat internal networks
- Weak MFA deployments
- Incomplete logging and monitoring programs

Cyber resilience increasingly depends on an organization’s ability to rapidly:

- Detect anomalous activity
- Isolate compromised systems
- Validate backups
- Patch critical vulnerabilities
- Enforce identity controls
- Monitor vendor exposure

Recommended Defensive Priorities

Immediate Priorities

- Enforce MFA across all remote and privileged access systems
- Reduce internet-facing attack surface exposure
- Conduct external vulnerability assessments
- Patch critical edge-device vulnerabilities rapidly
- Validate backup integrity and restoration procedures
- Review privileged account access and stale accounts

Mid-Term Priorities

- Implement centralized logging and SIEM visibility
- Deploy endpoint detection and response (EDR)
- Improve email security and phishing resilience
- Conduct tabletop incident response exercises
- Expand third-party risk assessments

Long-Term Priorities

- Adopt zero-trust architecture principles
- Mature identity governance programs
- Segment critical infrastructure and sensitive networks
- Improve cloud security posture management
- Integrate threat intelligence into security operations

Methodology

This assessment was compiled using:

- Public breach disclosures
- Open-source intelligence (OSINT)
- Ransomware leak monitoring
- Regulatory reporting datasets
- Public vulnerability intelligence
- Industry reporting and threat research

Data sources included:

- Federal breach reporting portals
- Cybersecurity advisories
- Public ransomware disclosures
- Industry incident reporting
- Open-source threat intelligence feeds

Geospatial analysis and visualization were conducted using Python-based workflows and QGIS mapping methodologies.

Disclaimer

This report reflects aggregated public cybersecurity reporting and is intended solely for informational and situational awareness purposes.

Inclusion of any organization, sector, or geographic area does not imply negligence, attribution, or fault. Publicly available datasets may not reflect the complete scope of cyber activity due to:

- Underreporting
- Delayed disclosure
- Regulatory limitations
- Ongoing investigations
- Private incident handling practices

Threat activity assessments are based on observed reporting trends available as of May 2026.

References

Cybersecurity and Infrastructure Security Agency. (n.d.). *Cybersecurity advisories and alerts*. U.S. Department of Homeland Security. https://www.cisa.gov/news-events/cybersecurity-advisories

Privacy Rights Clearinghouse. (n.d.). *Data breaches*. https://privacyrights.org/data-breaches

U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). *Breach portal: Notice to the Secretary of HHS breach of unsecured protected health information*. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Verizon. (n.d.). *Data breach investigations report (DBIR)*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Palo Alto Networks Unit 42. (n.d.). *Threat research and intelligence*. https://unit42.paloaltonetworks.com

Privacy Rights Clearinghouse. (n.d.). *Data breaches*. https://privacyrights.org/data-breaches

Recorded Future. (n.d.). *Threat intelligence resources*. https://www.recordedfuture.com/resources

Sophos. (n.d.). *State of ransomware report*. https://www.sophos.com/en-us/content/state-of-ransomware

CrowdStrike. (n.d.). *Global threat report*. https://www.crowdstrike.com/global-threat-report/

IBM. (n.d.). *IBM X-Force threat intelligence index*. https://www.ibm.com/reports/threat-intelligence