LastPass

Cyber Resilience Index (CRI)

for Emerging and Mid-Sized Companies:

A Quick Start Guide: Score it. Prove it. Improve it.

DR. CHASE CUNNINGHAM

The Origin and Rationale for the Cyber Resilience Index (CRI)

The Need for a New Model

Let’s be honest — the 1–5 maturity model has been a security industry comfort blanket for too long. You can score a ‘5’ and still get wrecked. What matters isn’t the shiny scorecard, it’s whether your business can take a punch and stay standing. That’s why the CRI exists.

Most security guidance stops at capability maturity — the classic 1–5 scale of how developed your controls are. While helpful, that approach has a central blind spot: it assumes perfect execution.

Breaches still happen even in “mature” environments, and the deciding factor in business survival isn’t just whether controls existed, but whether the business could recover quickly when they failed.

The Cyber Resilience Index (CRI) for emerging and mid-sized companies was designed to solve this gap. It’s not just about “Do you have MFA?” but “If MFA is bypassed, how much damage can be contained, and how fast can you return to normal operations?”

Behind the Build

Real-world breach cause data from high-credibility sources laid the foundation:

- **Verizon 2025 Data Breach Investigations Report (DBIR)** – provided the frequency of attack patterns by cause, broken down for smaller businesses vs. enterprises.
- **Coveware ransomware reports** – quantified the impact of backups, preparation, and incident response on ransom payment rates and downtime.
- **CrowdStrike Global Threat Report** – detailed the prevalence of “malware-free” intrusions, credential abuse, breakout times, and attacker tactics, techniques, and procedures (TTP).
- **Cybersecurity & Infrastructure Security Agency (CISA) and Zero Trust Maturity Model (ZTMM)** – informed control areas that map to current federal guidance.

The research dentified the five domains where the overwhelming majority of emerging and mid-sized company-impacting incidents occur:

- **Identity Assurance** – credential compromise was a top cause of breaches across DBIR categories, making identity security the single most leveraged attack vector for smaller firms.
- **Data Resilience** – ransomware prevalence (88% of smaller and mid-sized business breaches) makes backup, encryption, and recovery speed critical survival factors.
- **Threat Visibility** – detection delays drive impact; CrowdStrike data on breakout times (<1 hour) makes endpoint/network monitoring a necessity.
- **Vulnerability Velocity** – DBIR’s 34% YoY increase in vulnerability exploitation shows patch speed is as vital as patch coverage.
- **Supply Chain Security** – DBIR’s doubling of third party–origin breaches (now ~30%) makes partner/vendor security a real smaller business risk amplifier.

These domains were weighted based on relative frequency × average impact severity from DBIR and supporting reports, ensuring the CRI aligns with **where emerging and mid-sized companies are statistically most at risk.**

The Dual Scoring Concept

Don’t confuse maturity with survival. There are plenty of “mature” networks that end up in body bags after one phishing campaign. Resilience is what keeps the lights on. Think of it like boxing: maturity is your stance and guard. Resilience is whether you can recover when someone lands a clean shot. Most smaller companies only train for the stance, not the recovery.

Instead of only assigning a **Maturity Score** (1–5) to each domain, CRI also measures a **Resilience Factor** (0.0–1.0) — the realistic probability that the business will survive a major incident in that domain without catastrophic loss.

This approach is directly inspired by:

Business continuity research shows that post-breach survival depends as much on recovery time as on breach prevention.

Incident case studies from Coveware and Mandiant illustrate that businesses with high maturity but low resilience can still fail.

For example:

- A company with MFA everywhere but **no incident response plan** may still suffer catastrophic downtime after a credential phishing incident —
  Maturity: high; Resilience: low.
- Conversely, a growing business with average maturity but **bulletproof backups and tested failover** may bounce back from ransomware in hours —
  Maturity: mid; Resilience: high.

Why the CRI Is Evidence-Based and Actionable

The CRI is grounded in the most widely cited breach datasets in the industry (DBIR, CrowdStrike, Coveware) and designed to:

- Target the top 5 emerging and mid-sized company threat domains by prevalence and impact.
- Combine prevention and recovery in a single score.
- Be simple enough to calculate quarterly without consultants.
- Produce several metrics executives can track over time and link to ROI.

Because each domain is weighted by actual breach likelihood and impact severity, smaller companies using CRI aren't spending time on low-probability risks at the expense of high-impact gaps. This aligns directly with CISA's "risk-driven prioritization" guidance and NIST Cybersecurity Framework CSF's emphasis on outcome-based measurement.

A Framework You Can Own and Evolve

By branding and publishing the CRI, you establish a recognizable, repeatable emerging and mid-sized company security benchmark that can be:

- Released annually as an industry report.
- Used by MSPs, insurers, and business leaders as a quick health check.
- Enhanced over time with new threat vector weights as the landscape changes (e.g., AI-assisted phishing, deepfake fraud).

The CRI's strength is that it's both strategic and tactical:

- Strategic because it frames risk in terms of survival probability and business continuity.
- Tactical because it tells you exactly where to spend the next dollar for maximum CRI lift.

The Cyber Resilience Index (CRI) measures both your cybersecurity maturity and your ability to survive an attack. It focuses on five high-impact domains: Identity Assurance, Data Resilience, Threat Visibility, Vulnerability Velocity, and Supply Chain Security. Use this toolkit to score your business, visualize strengths/weaknesses, and plan improvements.

Purpose:

The CRI is a simple way to measure how ready your business is to survive a cyberattack — not just to prevent it. It combines:

Maturity – how strong your defenses are.

Resilience – how well you can recover if those defenses fail.

Step 1 – Score Each Domain

Rate yourself in **five critical areas** that account for most emerging and mid-size company breaches:

Domain	Examples of What's Included	Weight
Identity Assurance	MFA, password policies, credential monitoring	25%
Data Resilience	Backups, encryption, and tokenization	20%
Threat Visibility	Endpoint/network monitoring, 24/7 SOC/MDR	20%
Vulnerability Velocity	Patch speed, vulnerability scanning	20%
Supply Chain Security	Vendor risk reviews, breach notification clauses	15%

Maturity Score (1–5)

1 = Ad hoc / fundamental security

5 = Fully integrated, automated, and reviewed regularly

Resilience Factor (0.0–1.0)

Your realistic survival probability in that domain:

1.0 = Very likely to survive a major incident

0.5 = 50/50 chance

0.2 = Unlikely to survive without significant loss

Step 2 – Calculate CRI

Domain Score = Maturity × Resilience × Weight × 20

Add all 5 Domain Scores → CRI (0–500)

Score Ranges:

400–500: High Resilience – Strong defenses and recovery plans

300–399: Resilient but Evolving – Good in most areas, some gaps remain

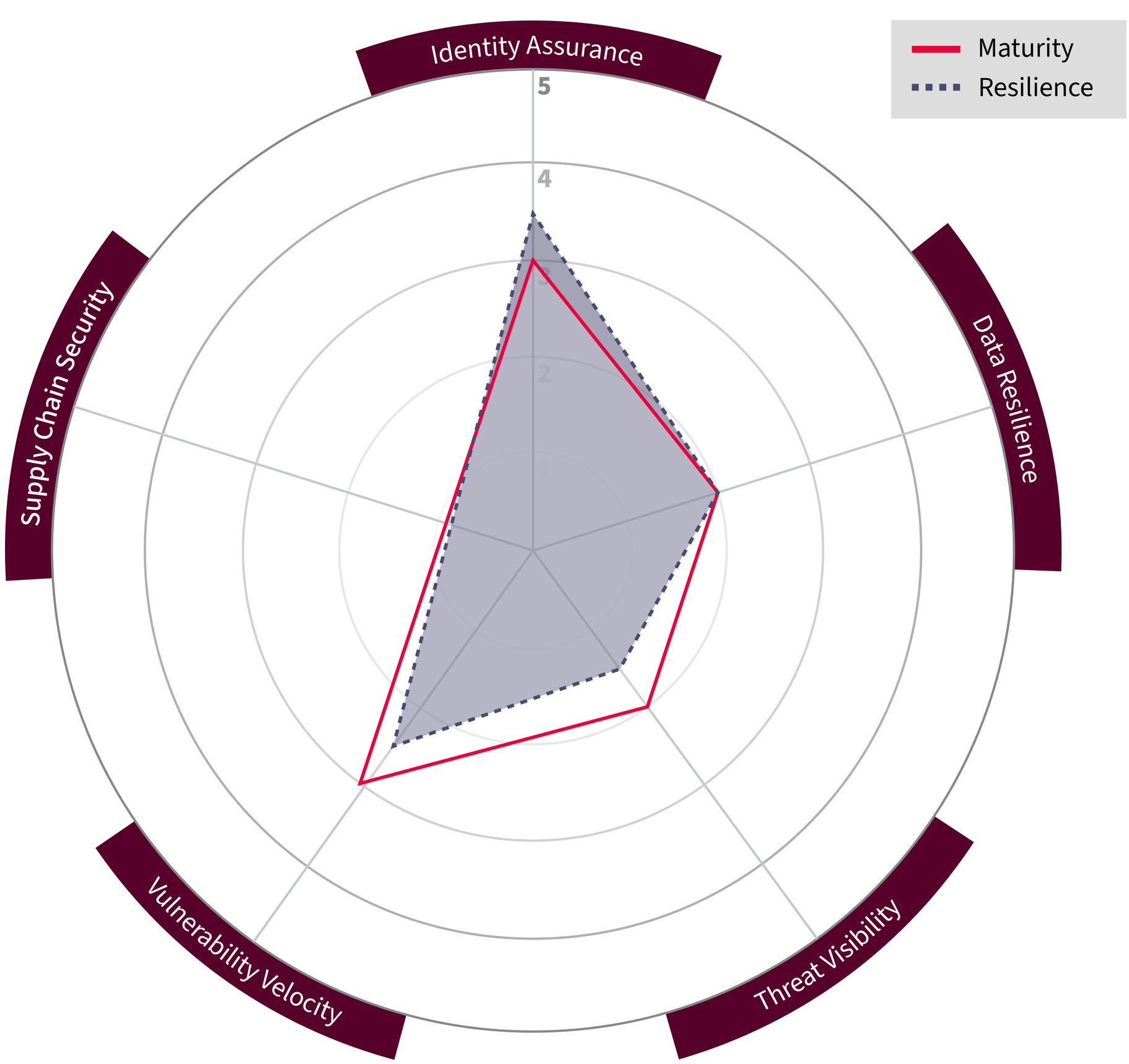
200–299: At Risk – Several weaknesses could be business-ending

Below 200: Vulnerable – Major overhaul needed

Step 3 – Visualize

Plot your **Maturity** and **Resilience** scores on a radar chart to see imbalances.

Cyber Resilience Index (CRI) Radar Chart



A balanced, outward-reaching shape is the goal.

Use this blank radar cart to plot your own maturity and resilience.

Download Chart

Step 4 – Take Action

Focus first on the **lowest-scoring domain** — raising that score often gives the most significant jump in CRI.

Typical fast wins:

- Use a password manager and set your minimum for the creation of new passwords to at least 12 characters with special characters and numbers
- Turn on MFA everywhere (Identity Assurance)
- Set up immutable cloud backups (Data Resilience)
- Add managed detection & response (Threat Visibility)
- Patch internet-facing systems first (Vulnerability Velocity)
- Add breach clauses to vendor contracts (Supply Chain Security)

Pro Tip: Recalculate your CRI quarterly to track improvement and justify your security budget. Cybersecurity isn't a one-and-done deal. Treat this like going to the gym. If you don't measure progress every quarter, you're just flexing in the mirror.

References

Verizon. (2025a). 2025 Data Breach Investigations Report: Executive summary. Verizon Business.

Verizon. (2025b). 2025 Data Breach Investigations Report (web page). Verizon Business.

CrowdStrike. (2025a). 2025 Global Threat Report. CrowdStrike Holdings, Inc. SecurityWeek

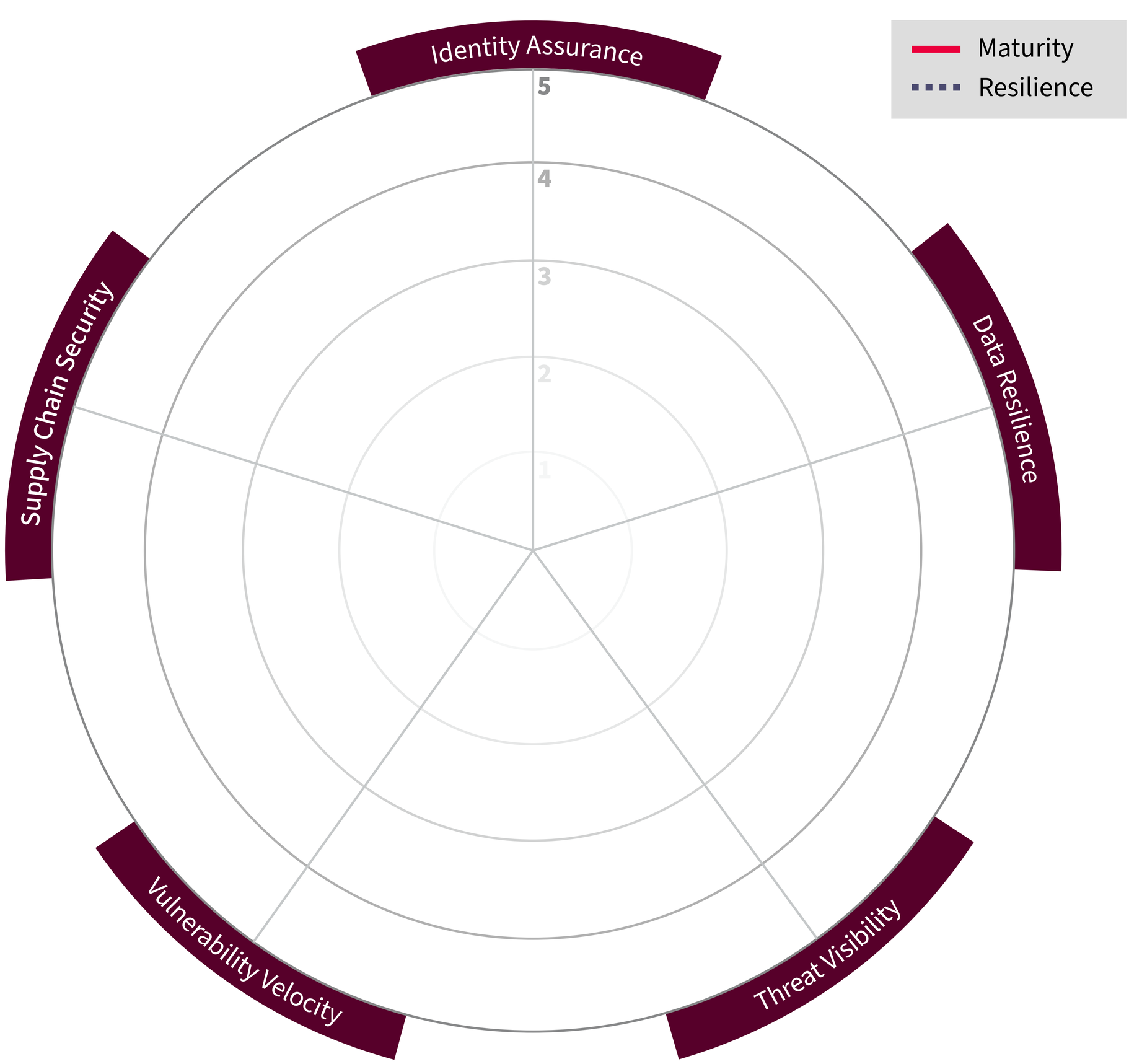
Coveware. (2025, January 31). Q4 Ransomware report.

CISA ZTMM Document – Cybersecurity & Infrastructure Security Agency. (2023, April). Zero Trust Maturity Model Version 2.0.

Download the full Cyber Resilience Playbook.

Plot your **Maturity** and **Resilience** scores on a radar chart to see imbalances.

Cyber Resilience Index (CRI) Radar Chart



A balanced, outward-reaching shape is the goal.