



How attackers actually got in.

A plain-language read of 2025 threat data, focused on what it means for Iowa small and mid-sized businesses.

THE VIEW FROM THE INSIDE

Only 1 in 3 smaller organizations stopped ransomware before it encrypted their data.

Among ransomware victims with 100 to 250 employees, just 34% caught the attack before encryption, and 43% said a lack of people or capacity contributed. Across all victims, an **unknown security gap** was the second most cited cause (36%).

The common breach isn't a nation-state operation. It is an organization that didn't know it was exposed and didn't have the hands to catch it.

Source: Sophos State of Ransomware 2026 (2,158 victims surveyed, Jan to Mar 2026).

HOW ATTACKERS GOT IN

Three entry points dominate. The ranking shuffles. The list doesn't.

Unpatched internet-facing systems. Exploitation started 31% of breaches in Verizon's data, overtaking stolen credentials for the first time. Firewalls, VPNs, and file-transfer apps (SonicWall, CrushFTP, Veeam, Gladinet) drove 2025's big waves. Only 26% of critical CISA-listed flaws were fully remediated.

Phishing and malicious email. Half of ransomware attacks in Sophos's survey started in the inbox. Microsoft remained the most imitated brand (22% of brand phishing, Q4 2025).

Stolen credentials. 79% of ransomware attacks were identity-based. MFA was present in 97% of credential-led incidents, so MFA alone is not the answer.

Sources: Verizon DBIR 2026 · Sophos State of Ransomware 2026 · Check Point Q4 2025 Brand Phishing.

WHY THIS BRIEF IS FOR SMBs

96% of ransomware victims were small and mid-sized businesses.

Verizon's data (22,000+ confirmed breaches) is unambiguous, and ransomware now appears in 48% of all breaches. Headlines focus on Fortune 500 breaches, but the population getting hit is overwhelmingly SMBs. Iowa's economy is built on that population.

Source: Verizon 2026 Data Breach Investigations Report.

IDENTITY IS THE NEW FRONT DOOR

Business Email Compromise drove \$3.05 billion in reported losses in 2025.

86% of that money moved by wire or ACH, about \$123,000 per complaint. BEC hits small finance teams without dual-approval controls hardest. In the common Iowa scenario, a vendor's email is taken over, wire instructions quietly change, and a routine-looking payment never reaches the real recipient.

Closer to home. Iowans filed 5,436 complaints and reported \$95.5 million in losses. Iowa had the fewest complaints per capita of any state. A low reporting rate is not a low attack rate.

Source: FBI IC3 2025 Internet Crime Report (released April 2026).

SPEED VERSUS DETECTION

Attackers move in hours. Most breaches go unnoticed for months.

The average time from an attacker's first foothold to ransomware was **20 hours**, up from 17 as crews linger to steal data. The mean time to identify and contain a breach was **247 days**, up from 241 and the first rise in five years.

That gap, hours to do harm and months to notice, is the real exposure. A clean perimeter and a current patch list are necessary. They are not sufficient.

Sources: Huntress 2026 Cyber Threat Report (time-to-ransom) · IBM Cost of a Data Breach 2026 (MTTI + MTTC).