MANAGED IT & CYBERSECURITY SERVICES

2026 ANNUAL
CYBERSECURITY THREAT REPORT

What Small & Mid-Sized Businesses Need to Know About Ransomware, AI-Driven Phishing, and Emerging Risk in 2026 and What to Expect in 2027

We Manage Your IT. You Manage Your Business.

Prepared by ICSI | www.icsi.com

Compiled using data from the Verizon Data Breach Investigations Report, IBM Cost of a Data Breach Report, FBI Internet Crime Complaint Center (IC3), Datto, and other leading industry sources.

Executive Summary

Cybercrime against small and mid-sized businesses accelerated sharply through 2025 and into 2026. Ransomware now touches nearly half of all confirmed data breaches, the highest share ever recorded — and generative AI has fundamentally changed the economics of phishing and social engineering, making sophisticated attacks cheap and easy to launch at scale.

This report compiles the most significant, well-documented cybersecurity trends affecting businesses nationwide heading into 2027, drawing on leading industry research including the Verizon Data Breach Investigations Report (DBIR), IBM's Cost of a Data Breach Report, the FBI's Internet Crime Complaint Center (IC3), and other primary sources. Our goal is simple: to give business owners and IT leaders a clear, jargon-free picture of the risks that matter most right now and practical steps to address them.

48%

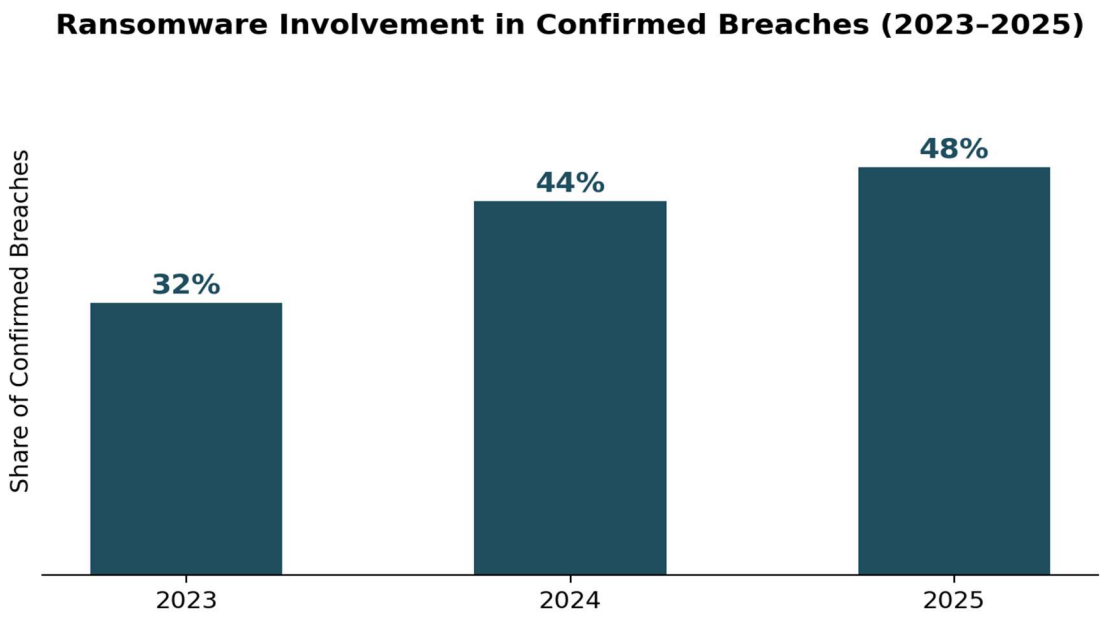
of confirmed data breaches in 2025 involved ransomware — the highest share in the 19-year history of the Verizon DBIR

A Note on Our Sources

The statistics in this report are drawn from established, publicly available industry research rather than proprietary survey data. Where a figure comes from a specific study, we've cited it directly. ICSI plans to field its own nationwide survey of business IT decision-makers in the coming year to supplement this analysis with original, ICSI-specific data in future editions of this report.

1. The Ransomware Epidemic Isn't Slowing Down

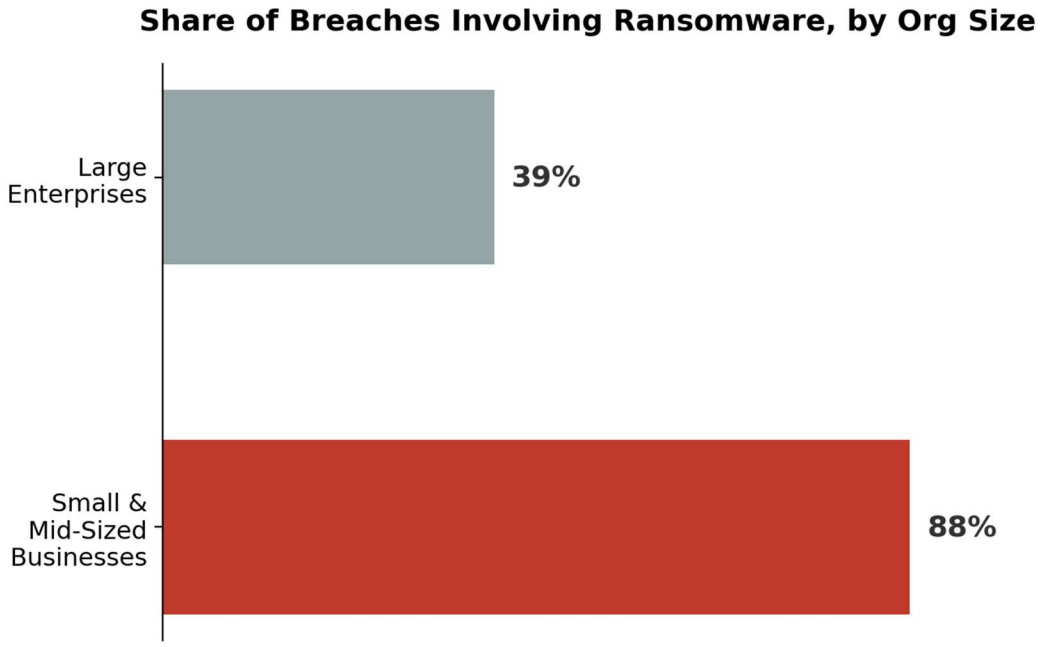
Ransomware remains the single most consequential threat facing businesses today. According to the Verizon 2026 Data Breach Investigations Report, which analyzed more than 31,000 security incidents across 14 industries, ransomware was involved in 48% of confirmed breaches in 2025, up from 44% the year before. It's a trend line that has climbed in every edition of the report for years running.



Source: Verizon 2026 Data Breach Investigations Report

Small Businesses Bear the Brunt

Ransomware operators have increasingly shifted their focus toward smaller organizations, which typically have weaker defenses, less dedicated security staff, and fewer resources to recover quickly. Industry data suggests that among ransomware incidents where the victim's size was known, small and mid-sized businesses accounted for the overwhelming majority.



Source: Verizon 2026 DBIR / Datto Global State of the Channel Ransomware Report

Attackers favor smaller targets not because the payouts are larger, but because the odds of success are. Weaker patching practices, limited monitoring, and reliance on a single generalist IT resource (rather than a dedicated security team) all make small and mid-sized businesses a comparatively easy and reliable source of revenue for ransomware-as-a-service (RaaS) operations.

2. AI Has Changed the Economics of Phishing

Generative AI has removed the traditional tells that once made phishing emails easy to spot, awkward phrasing, obvious grammatical errors, and generic messaging. Attackers now use AI tools to research targets, mimic writing styles, and generate polished, personalized lures in seconds rather than hours.

- Spear phishing content linked to generative AI has surged dramatically since 2023, with multiple industry trackers reporting increases well into the quadruple digits year-over-year.
- AI-generated phishing messages have been shown in controlled research (including a University of Oxford study) to achieve dramatically higher click-through rates than traditionally written phishing emails.
- Voice phishing ("vishing") using AI-generated voice cloning and deepfake technology has also grown sharply, adding a new and difficult-to-detect vector for social engineering attacks.

The practical impact for businesses: employee security awareness training built around "spotting bad grammar" is now largely obsolete. Training needs to shift toward behavioral red flags, unusual urgency, unexpected payment requests, and out-of-process approval asks, regardless of how polished the message looks.

3. Business Email Compromise: The Costliest Threat Category

Business Email Compromise (BEC), in which an attacker impersonates an executive, vendor, or trusted colleague to redirect payments or extract sensitive information, continues to be one of the most financially damaging categories of cybercrime reported to federal authorities.

$3.0B+

in reported losses from Business Email Compromise incidents tracked by the FBI's Internet Crime Complaint Center in its most recent annual report

BEC is particularly dangerous because it requires no malware and no technical exploit, just a convincing impersonation and a routine-looking request. That makes it very difficult for traditional

security tools to catch, and it places the burden of detection on employees, particularly those in finance and accounts payable roles who are accustomed to processing payment requests quickly.

4. Why Small & Mid-Sized Businesses Remain the Primary Target

Several consistent factors explain why smaller organizations continue to be disproportionately targeted:

- Limited or no dedicated cybersecurity staff, many small businesses rely entirely on a single generalist IT resource or outsource reactively rather than proactively.
- Outdated systems and inconsistent patching, often due to budget constraints or lack of a formal update cadence.
- Heavier reliance on third-party vendors and managed providers, which, without proper oversight, can introduce supply-chain risk.
- A persistent perception gap: many small business leaders still believe they're "too small to be a target," when in fact the data shows the opposite is true.

Attackers increasingly treat small and mid-sized businesses as an efficient, high-volume revenue channel, not an afterthought.

5. The Emerging Risk: Shadow AI in the Workplace

Beyond traditional attack vectors, a newer and less understood risk is emerging from within organizations themselves: employees using unsanctioned, consumer-grade AI tools to handle sensitive business data, often without IT's knowledge or any governing policy in place.

Unlike a phishing email or ransomware payload, shadow AI isn't an external attack, it's a governance gap. Client data, financial records, proprietary code, and even regulated information (like patient records in healthcare settings) are increasingly being entered into public AI tools by well-meaning employees looking for a shortcut. Once that data leaves the organization’s-controlled environment, there's no way to know how it's stored, retained, or used.

As AI tool adoption continues to outpace formal governance at most organizations, we expect shadow AI to become one of the most significant, and most overlooked, data security risks of 2027.

2027 Outlook: What to Expect

- Ransomware involvement in confirmed breaches will likely continue climbing, with small and mid-sized businesses remaining the primary target for RaaS operators.
- AI-generated social engineering, email, voice, and eventually video-based deepfakes, will become a standard part of the attacker toolkit rather than a novel tactic.

- Regulatory scrutiny of AI data handling practices will increase, particularly in healthcare, financial services, and legal sectors, raising the compliance stakes for shadow AI usage.
- Businesses without a formal, tested incident response plan will face longer recovery times and higher costs relative to those with one in place.
- Third-party and vendor risk will continue to grow as a breach vector, making vendor security vetting an increasingly essential, not optional, part of a business's security posture.

Recommendations for Business Leaders

1. Assume You're a Target

The data is unambiguous: small and mid-sized businesses are targeted at least as often as, and by some measures more often than large enterprises. Security planning should start from that assumption, not from "it won't happen to us."

2. Modernize Security Awareness Training

Training built around spotting typos and bad grammar no longer reflects the threat. Employees need training focused on behavioral red flags and verification habits, especially around payment requests and credential changes.

3. Establish an AI Usage Policy

Most organizations still lack any formal governance around employee AI tool usage. A clear policy, paired with an approved, secure AI alternative, closes one of the fastest-growing data risk gaps without banning tools employees genuinely find useful.

Outsource 24/7 Monitoring

Ransomware and BEC attacks often succeed simply because no one is watching after hours. Continuous monitoring, whether built in-house or through a managed security partner, significantly reduces dwell time and limits damage.

5. Test Your Incident Response Plan Before You Need It

A response plan that has never been tested is a plan in name only. Regular tabletop exercises reveal gaps in communication, roles, and recovery procedures long before a real incident does.

6. Vet Third-Party and Vendor Access

As breaches increasingly originate through third parties, businesses need clear visibility into which vendors have access to their systems and data, and what security standards those vendors are held to.

How ICSI Can Help

ICSI partners with businesses nationwide to build practical, right-sized cybersecurity and managed IT programs from 24/7 threat monitoring and incident response planning to AI governance and employee security awareness training. Whether you're building a security program from scratch or strengthening an existing one, our team can help you understand exactly where your organization stands today and what to prioritize next.

Contact ICSI today for a complimentary cybersecurity risk assessment. Call 410-280-3000 or visit our website at www.icsi.com

Sources

Verizon. 2026 Data Breach Investigations Report.

IBM Security. Cost of a Data Breach Report 2025.

Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). 2025 Internet Crime Report.

Datto. Global State of the Channel Ransomware Report.

KnowBe4. 2025 Phishing Threat Trends Report.

University of Oxford research on AI-generated phishing click-through rates, as cited in industry press.

This report reflects publicly available third-party research current as of publication and is provided for general informational purposes. It does not constitute legal, compliance, or professional security advice specific to any organization.