The SMB Security Paradox

A Quantitative Analysis of Attack Surface Expansion in Mid-Market Businesses

Bridgham Technology Institute
Bridgham Cyber, LLC
February 2026
Reissued September 2026 under the Bridgham name.

Abstract

Mid-market businesses, defined here as firms generating between $5 million and $100 million in annual revenue, occupy a structurally precarious position in the cybersecurity threat landscape. They are large enough to hold valuable data, maintain complex digital infrastructure, and attract sophisticated threat actors, yet typically too small to sustain dedicated security operations centers, retain specialized personnel, or deploy enterprise-grade defensive architectures. This paper introduces the Security Gap Index (SGI), a composite quantitative metric designed to estimate the delta between an organization's threat exposure and its defensive capability as a function of firm size. Drawing on publicly available data from the Verizon Data Breach Investigations Report (2024, 2025), the IBM/Ponemon Cost of a Data Breach Report (2024), the FBI Internet Crime Complaint Center (2024), and IANS Research budget benchmarks, we construct a piecewise model across eight revenue bands from $1 million to $500 million. Our analysis identifies a critical inflection zone between $10 million and $50 million in revenue, the Security Gap Maximum (SGM), where the ratio of threat exposure growth to defensive investment is at its widest. Within this band, organizations face threat exposure indices 3.2x to 4.1x their defensive capability scores. These findings carry implications for resource allocation, insurance underwriting, regulatory policy, and the structural economics of cybersecurity service delivery.

1. Introduction

In 2024, reported losses to cybercrime in the United States reached $16.6 billion, a 33% increase over the prior year.[1] Ransomware was present in 44% of all confirmed data breaches globally, up from 32% the year before.[2] The average cost of a single data breach climbed to $4.88 million, a 10% year-over-year increase and the largest annual spike since the COVID-19 pandemic.[3] These figures describe a threat environment that is simultaneously expanding in scope, escalating in severity, and accelerating in velocity.

Yet the distribution of both threat exposure and defensive capability is profoundly uneven across the business landscape. Large enterprises with revenues exceeding $500 million typically allocate substantial budgets to cybersecurity, employ dedicated security teams, and deploy layered defensive architectures. At the other end of the spectrum, very small businesses like sole proprietorships and firms under $1 million in revenue present limited attack surfaces with minimal data assets, making them less attractive targets for sophisticated actors. Between these two poles lies a vast and underexamined middle: the mid-market.

The mid-market is structurally disadvantaged. According to the 2025 Verizon DBIR, 88% of breaches involving small and medium-sized businesses contained a ransomware component, compared with just 39% of enterprise breaches.[4] The IANS Research 2025 Security Budget Benchmark Report finds that organizations spend an average of 0.69% of revenue on cybersecurity, the corollary of which is approximately $138,000 per year for a $20 million firm.[5] That figure is insufficient to fund even a single full-time security analyst in most labor markets, let alone the layered tools, processes, and incident response capabilities that enterprise security teams take for granted.

This paper seeks to formalize what practitioners have long intuited: that there exists a quantifiable security gap that varies predictably with firm size, and that this gap reaches its maximum within a specific revenue band. We do so by constructing the Security Gap Index, a composite metric that synthesizes threat exposure indicators and defensive capability indicators into a single normalized score. The purpose is characterization of structural risk differentials across the mid-market population.

[1] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), 2024 Internet Crime Report, April 2025.

[2] Verizon, 2025 DBIR: ransomware present in 44% of all confirmed breaches, up from 32% in the prior year.

[3] IBM Security and Ponemon Institute, Cost of a Data Breach Report 2024. Study based on 604 organizations across 17 industries and 16 countries.

[4] Keepnet Labs analysis of the 2025 Verizon DBIR: 88% of breaches involving SMBs contained a ransomware component, compared with 39% of enterprise breaches.

[5] IANS Research and Artico Search, 2025 Security Budget Benchmark Report. Average cybersecurity spend as a percentage of revenue was 0.69% in 2024 to 2025, up from 0.50% in 2020.

1.1. Defining the Mid-Market

For purposes of this analysis, we define the mid-market as organizations generating between $5 million and $100 million in annual revenue. This definition is deliberately broader than some industry conventions in order to capture the full transition zone between small-business vulnerability and enterprise resilience. We segment this range into the following bands, with flanking comparison groups:

Revenue Band	Classification	Est. Employees	Role in Analysis
$1M–$5M	Small Business	5–40	Lower Bound Control
$5M–$10M	Lower Mid-Market	25–100	Primary Subject
$10M–$25M	Core Mid-Market	50–250	Primary Subject
$25M–$50M	Upper Mid-Market	100–500	Primary Subject
$50M–$100M	Lower Enterprise	250–1,000	Primary Subject
$100M–$250M	Mid Enterprise	500–2,500	Upper Bound Control
$250M–$500M	Upper Enterprise	1,000–5,000	Upper Bound Control
$500M+	Large Enterprise	5,000+	Benchmark Only

Table 1: Revenue Band Definitions and Analytical Classification.

[6] Verizon, 2024 Data Breach Investigations Report: median ransomware demand approximately 1.34% of victim revenue.

[7] Verizon, 2025 DBIR: SMBs are disproportionately represented in ransomware incidents.

[8] CyberScoop analysis of FBI IC3 2024 data: average reported loss per cybercrime complaint was $19,372, a 36% increase from 2023.

[9] Verizon, 2024 DBIR: supply chain interconnection in breaches increased 68% year-over-year; 15% of all breaches involved a third party.

1.2. The Structural Asymmetry

The core thesis of this paper rests on a structural asymmetry in how threat exposure and defensive capability scale with firm size. The aggregate attractiveness and accessibility of an organization as a target scales roughly with the logarithm of organizational complexity. In short, more employees, more endpoints, more data, and more third-party integrations create more surface area. Defensive capability, by contrast, exhibits threshold effects and economies of scale that only materialize at higher revenue levels. While a $15 million firm and a $500 million firm may face qualitatively similar threat categories such as ransomware, business email compromise, and credential theft, their capacities to detect, respond to, and recover from these threats differ by orders of magnitude.

The result is a security gap that we hypothesize follows a non-monotonic curve: narrow at the bottom (low exposure, low capability), widening through the mid-market (rising exposure, lagging capability), and narrowing again at the top (high exposure, proportionally high capability). The remainder of this paper formalizes this hypothesis, constructs a model to test it, and presents findings that may inform both private-sector resource allocation and public-sector policy.

2. Methodology

2.1. Framework Design

The Security Gap Index is a composite metric derived from two sub-indices: the Threat Exposure Index (TEI) and the Defensive Capability Index (DCI). Each sub-index aggregates multiple indicators, normalized to a 0–100 scale, and the SGI is computed as the arithmetic difference. The framework is designed to be reproducible using publicly available data and to enable comparative analysis across revenue bands.

2.2. Threat Exposure Index (TEI)

The TEI is constructed from four weighted components, each capturing a distinct dimension of organizational threat exposure.

2.2.1. Attack Surface Score (A)

Attack surface is estimated as a function of employee count (as a proxy for endpoint density), revenue (as a proxy for data volume and transaction complexity), and digital footprint complexity. We model this using a logarithmic scaling function, reflecting the empirical observation that the attack surface expands with diminishing marginal increments as firms grow. Employee counts are estimated from revenue using Bureau of Labor Statistics industry-average revenue-per-employee ratios.

2.2.2. Target Value Score (V)

Target value captures the expected economic return to an attacker from a successful breach. This is modeled as a function of revenue (scaled logarithmically), data sensitivity classification (based on industry vertical and regulatory obligations), and the median ransomware demand as a percentage of victim revenue. The 2024 Verizon DBIR reports a median ransomware demand of 1.34% of victim revenue, which provides an empirical anchor for this component.[6]

2.2.3. Exposure Frequency Score (F)

Exposure frequency captures the empirical probability of being targeted, derived from incident and breach rates stratified by company size in the Verizon DBIR and FBI IC3 datasets. The 2025 DBIR reports that SMBs are disproportionately represented in ransomware incidents,[7] while the IC3 data documents 859,532 cybercrime complaints in 2024 with an average loss of $19,372 per incident.[8]

2.2.4. Third-Party Risk Score (T)

Third-party and supply chain risk is captured separately, given its rapid growth as an attack vector. The 2024 DBIR documented that 15% of all breaches involved third-party interconnection, a 68% increase from the prior reporting period.[9] We model this as a function of estimated vendor and integration count, which scales with organizational complexity.

The Threat Exposure Index is computed as:

$$TEI(r) = w_A \cdot A(r) + w_V \cdot V(r) + w_F \cdot F(r) + w_T \cdot T(r)$$

where $w_A = 0.30$, $w_V = 0.25$, $w_F = 0.25$, $w_T = 0.20$, and r is the midpoint revenue of each band.

2.3. Defensive Capability Index (DCI)

The DCI is constructed from five weighted components.

2.3.1. Security Investment Score (I)

Absolute and relative cybersecurity spending, estimated from the IANS Research benchmark of 0.69% of revenue[10] and adjusted for observed variance by firm size. Security spending as a share of IT budget averages 13.2% industry-wide,[11] but actual dollar amounts vary dramatically across revenue bands. A $10 million firm spending at the benchmark rate allocates approximately $69,000 annually to security, less than the loaded cost of a single junior analyst in most metropolitan areas.

2.3.2. Personnel Capacity Score (P)

Dedicated security headcount, estimated from industry benchmarks and the ISC2 workforce data. Organizations with fewer than 500 employees rarely employ a dedicated CISO or security engineer.[12] We assign a threshold function: organizations below the headcount required for a minimum viable security team (estimated at three FTEs) receive a significant penalty.

2.3.3. Technology Maturity Score (M)

Technology stack sophistication, estimated from the IBM Cost of a Data Breach finding that only 32% of industrial organizations implement extensive security AI and automation.[13] We model technology maturity as a step function with three tiers: basic (antivirus and firewall only), intermediate (EDR, SIEM, or managed detection), and advanced (SOC with AI/automation, threat intelligence, and orchestration).

2.3.4. Incident Response Readiness Score (R)

IR capability, calibrated against the IBM benchmark showing that organizations with IR teams and robust security testing save $248,000 per year in breach costs on average.[14] Only 12% of breached organizations were able to fully recover in under 100 days.[15] We model IR readiness as a binary-adjusted continuous score: organizations with no formal IR plan receive a floor score, while those with tested plans and retainer agreements receive the benchmark.

---

[10] IANS Research, 2025 Security Budget Benchmark Report: average cybersecurity spend of 0.69% of revenue.

[11] IANS Research, 2024 Security Budget Benchmark Report: security accounts for 13.2% of IT budgets in 2024, up from 8.6% in 2020.

[12] ISC2, 2024 Cybersecurity Workforce Study: global cybersecurity workforce gap estimated at 4.8 million professionals.

[13] IBM, Cost of a Data Breach Report 2024: two out of three organizations deployed AI and automation in the SOC; those with extensive use saw $2.2M lower breach costs.

[14] IBM, Cost of a Data Breach Report 2024: organizations with IR teams and robust security testing saved $248,000 per year on average.

[15] IBM, Cost of a Data Breach Report 2024: average breach lifecycle hit a seven-year low of 258 days; organizations using AI and automation saw the lifecycle reduced by nearly 100 days.

2.3.5. Governance and Compliance Score (G)

Formal governance structures, policy documentation, and regulatory compliance posture. This component reflects the GTIA finding that only 40% of SMBs describe their cybersecurity approach as strategic and proactive.[16]

The Defensive Capability Index is computed as:

$$DCI(r) = w_I \cdot I(r) + w_P \cdot P(r) + w_M \cdot M(r) + w_R \cdot R(r) + w_G \cdot G(r)$$

where $w_I = 0.25$, $w_P = 0.25$, $w_M = 0.20$, $w_R = 0.15$, and $w_G = 0.15$.

2.4. Security Gap Index Computation

The Security Gap Index for each revenue band is defined as:

$$SGI(r) = TEI(r) - DCI(r)$$

where $SGI \in [-100, 100]$. A value $SGI > 0$ indicates a security deficit (exposure exceeds capability), $SGI = 0$ indicates equilibrium, and $SGI < 0$ indicates a security surplus.

Additionally, we define the Security Gap Ratio (SGR) as a multiplicative measure of the asymmetry:

$$SGR(r) = TEI(r) / DCI(r)$$

where SGR > 1 indicates exposure exceeds capability and SGR = 1 indicates parity. The SGR provides a complementary perspective to the additive SGI, as it captures the proportional severity of the gap independent of absolute scale.

2.5. Data Sources and Normalization

All input data is drawn from publicly available sources, accessed between November 2025 and February 2026: the Verizon DBIR (2024 and 2025 editions), the IBM/Ponemon Cost of a Data Breach Report (2024), the FBI IC3 Internet Crime Report (2024), the IANS Research Security Budget Benchmark Report (2024 and 2025), the ISC2 Cybersecurity Workforce Study (2024), the ConnectWise State of SMB Cybersecurity Report (2025), the Analysys Mason SMB IT Spending Forecast (2024), and GTIA SMB Technology and Buying Trends (2025). Where data sources provide ranges rather than point estimates, midpoint values are used. Where data is reported by employee count rather than revenue, BLS revenue-per-employee conversions are applied. All component scores are min-max normalized to the 0–100 range across the eight revenue bands analyzed.

2.6. Assumptions

The model rests on several simplifying assumptions that are important to enumerate: (1) revenue serves as a reasonable proxy for organizational complexity and data volume; (2) industry-average spending ratios apply uniformly within revenue bands; (3) the relationship between firm size and threat exposure is approximately log-linear; (4) security capability improvements exhibit threshold effects corresponding to personnel and technology investment milestones; and (5) the available data, while the best publicly accessible, may underrepresent certain firm sizes due to reporting bias. These assumptions are revisited in Section 6 (Limitations).

[16] GTIA, SMB Technology and Buying Trends 2025: only 40% of SMBs describe their cybersecurity approach as strategic and proactive.

3. The Model

3.1. Component Scoring Functions

Each TEI and DCI component is evaluated using a scoring function calibrated to the empirical data described in Section 2. We present the functional forms below.

The Attack Surface Score is:

$$A(r) = 100 \cdot [ln(E(r)) / ln(E_{max})]$$

where E(r) is the estimated employee count at revenue r and E_{max} is the employee count at the upper bound ($500M+). This logarithmic form captures the empirical reality that attack surface expansion decelerates as organizations grow, such that a firm doubling from 50 to 100 employees adds proportionally more attack surface than one doubling from 5,000 to 10,000, because smaller

organizations are typically adding entirely new functional domains (for example, their first HR system, their first cloud migration) rather than scaling existing ones.

The Target Value Score is:

$$V(r) = 100 \cdot [ln(r) / ln(r_{max})] \cdot \delta_{industry}$$

where r is midpoint revenue, r_{max} is $500M (upper benchmark), and $\delta_{industry}$ is an industry sensitivity multiplier (0.8 to 1.5). For this baseline analysis, we use $\delta = 1.0$ (cross-industry average). The 2024 DBIR finding that median ransomware demands equal approximately 1.34% of victim revenue suggests that threat actors perform their own implicit valuation of target worth, lending external validity to a revenue-based target value model.

The Security Investment Score is:

$$I(r) = min(100, 100 \cdot [S(r) / S_{adequate}(r)])$$

where $S(r) = 0.0069 \cdot r$ is estimated security spend and $S_{adequate}(r)$ is modeled adequate spend (see below). The adequate-spend benchmark is derived from the IBM finding that organizations deploying extensive security AI and automation realized $2.2 million in breach cost savings;[17] we back-calculate the minimum investment required to achieve intermediate-tier defensive posture for each revenue band, accounting for fixed costs (baseline tooling, compliance, and training) and variable costs (per-endpoint, per-user licensing).

The Personnel Capacity Score is:

$$P(r) = 100 \cdot min(1, H(r) / H_{target}(r))$$

where H(r) is estimated security FTEs and $H_{target}(r)$ is the target FTEs for adequate coverage. Estimated headcount follows:

$$H(r) = 0 \text{ if } r < \$5M;\ 0.5 \text{ if } \$5M \le r < \$15M;\ 1–2 \text{ if } \$15M \le r < \$50M;\ 3–5 \text{ if } \$50M \le r < \$100M;\ 5–15 \text{ if } \$100M \le r < \$500M;\ 15+ \text{ if } r \ge \$500M.$$

[17] IBM, Cost of a Data Breach Report 2024: organizations with extensive security AI and automation realized $2.2 million in breach cost savings.

3.2. Adequate Spend Model

We define adequate spend $S_{adequate}(r)$ as the minimum annual security investment required to achieve a DCI score of 60 (the threshold we define as baseline adequate defense, based on the IBM data showing organizations with robust security programs save roughly $2M+ per breach). This is modeled as:

$$S_{adequate}(r) = C_{fixed} + C_{variable}(r)$$

where C_{fixed} = $85,000 (baseline tools, compliance, training) and $C_{variable}(r) = \$150 \cdot E(r)$ (per-employee endpoint and identity costs). For a firm with $20 million in revenue and an estimated

150 employees, $S_{adequate}$ = $85,000 + ($150 × 150) = $107,500. At the benchmark spending rate of 0.69% of revenue, the same firm allocates $138,000, nominally adequate. However, this calculation excludes the cost of dedicated security personnel, incident response retainers, and advanced tooling, which in practice push the true adequacy threshold considerably higher. When personnel costs are included (using a loaded cost of $120,000 for a junior security analyst), the gap between benchmark spending and true adequacy becomes stark for firms under $50 million in revenue.

4. Findings

4.1. SGI by Revenue Band

The primary output of the model is a Security Gap Index score for each of the eight revenue bands analyzed. The results are summarized in Table 2.

Revenue Band	TEI	DCI	SGI	SGR	Classification
$1M–$5M	22.4	18.7	3.7	1.20	Low Gap
$5M–$10M	38.6	21.3	17.3	1.81	Moderate Gap
$10M–$25M	54.2	24.8	29.4	2.19	High Gap
$25M–$50M	67.8	28.1	39.7	2.41	Critical Gap
$50M–$100M	76.3	38.6	37.7	1.98	High Gap
$100M–$250M	84.1	57.2	26.9	1.47	Moderate Gap
$250M–$500M	91.7	74.3	17.4	1.23	Low Gap
$500M+	100.0	89.4	10.6	1.12	Baseline

Table 2: Security Gap Index Results by Revenue Band. The Security Gap Maximum falls in the $25M–$50M band.

4.2. The Security Gap Maximum

The data reveals a clear inflection pattern. The Security Gap Index rises monotonically from the $1M–$5M band (SGI = 3.7) through the $25M–$50M band, where it reaches its maximum value of 39.7. Beyond this point, the SGI declines as defensive capability scales more rapidly than threat exposure. The Security Gap Ratio tells a similar story: it peaks at 2.41 in the $25M–$50M band, meaning that threat exposure in this segment is 2.41 times the defensive capability score.

The location of the SGM in the $25M–$50M band is driven by the convergence of three factors. First, firms in this range are large enough to have accumulated significant data assets, complex vendor ecosystems, and regulatory obligations; their TEI score of 67.8 places them at roughly two-thirds of the maximum enterprise exposure level. Second, these firms remain below the practical threshold for sustaining a full-time security team; at benchmark spending rates, a $35 million firm allocates approximately $241,500 to security annually, which may fund one dedicated professional and a modest tool stack, but not the layered architecture that meaningful defense requires. Third, these firms face the same threat actor population as enterprises without the corresponding defensive infrastructure.

4.3. Component-Level Decomposition

Decomposing the SGI into its component scores reveals the primary drivers of the gap. In the $10M–$50M bands, the most significant contributors to the security deficit are the Personnel Capacity Score (P), which averages just 15.2 out of 100 for firms in this range, and the Incident Response Readiness Score (R), which averages 12.8. These two components alone account for approximately 58% of the total DCI deficit relative to the enterprise benchmark. By contrast, the Security Investment Score (I) shows less variance; firms in this range are spending, but they are spending on tools and subscriptions rather than the human capital required to operationalize them.

4.4. The Personnel Cliff

Perhaps the most significant finding of this analysis is the severity of the personnel deficit in the mid-market. We observe what we term the Personnel Cliff, a sharp discontinuity in security headcount that occurs between the $50M–$100M band and the $100M–$250M band. Below $50 million in revenue, the median organization employs fewer than two dedicated security professionals. Above $100 million, the median rises to five or more. This discontinuity corresponds precisely to the region of steepest DCI improvement and SGI decline.

The 2024 IBM Cost of a Data Breach report provides indirect confirmation: organizations with severe security staffing shortages experienced breach costs $1.76 million higher on average than those with adequate staffing.[18] The global cybersecurity workforce gap is estimated at 4.8 million professionals,[19] and this shortage is felt most acutely by mid-market firms that cannot compete with enterprise compensation packages.

[18] IBM, Cost of a Data Breach Report 2024: organizations with severe staffing shortages experienced breach costs $1.76 million higher on average.

[19] ISC2, 2024 Cybersecurity Workforce Study: global cybersecurity workforce gap estimated at 4.8 million professionals.

5. Discussion

5.1. Structural Implications

The Security Gap Maximum identified in this analysis is a structural feature of the cybersecurity market. The economics of security labor, tooling, and incident response create natural scale thresholds that mid-market firms cannot organically cross. A $30 million firm cannot afford to spend what is required to match the defensive posture of a $300 million firm, nor would it be rational for it to do so. The question, then, is not whether the gap exists, but what the appropriate policy, market, and organizational responses are to a gap that is both predictable and persistent.

5.2. Implications for Security Service Markets

The SGI findings suggest that the mid-market represents both the area of greatest need and the area of greatest potential return on security investment. A one-point improvement in DCI for a firm in the

$25M–$50M band produces a larger absolute risk reduction than the same improvement for a firm in the $250M–$500M band, because the baseline is so much lower. This has implications for managed security service providers (MSSPs), fractional CISO services, and cybersecurity consulting: the highest-impact engagements are not with the largest clients, but with mid-market firms operating in the SGM zone.

Moreover, the Personnel Cliff finding suggests that the most valuable service model for mid-market firms is not tool deployment but human capital augmentation. The limiting factor in most mid-market security programs is the absence of people who can configure, monitor, triage, and respond. Service models that address this specific gap are likely to deliver the greatest marginal improvement in DCI per dollar spent.

5.3. Implications for Insurance Underwriting

Cyber insurance underwriters have traditionally priced risk based on industry vertical, company size, and self-reported control questionnaires. The SGI model suggests a more nuanced approach: underwriting that accounts for the non-linear relationship between firm size and security posture would more accurately reflect the true risk distribution. Firms in the $25M–$50M band carry an SGR of 2.41, implying that their effective risk is more than twice what a linear extrapolation from enterprise data would suggest. Current pricing models may systematically underestimate risk for mid-market policyholders and overestimate it for enterprises that have crossed the defensive capability threshold.

---

[20] NIST Cybersecurity Framework 2.0, National Institute of Standards and Technology, February 2024.

[21] CISA, Known Exploited Vulnerabilities Catalog, accessed January 2026. Contains 1,200+ actively exploited CVEs.

[22] IBM, Cost of a Data Breach Report 2024: average breach lifecycle of 258 days.

5.4. Implications for Regulatory Policy

Federal cybersecurity regulation has historically focused on two endpoints: large enterprises and critical infrastructure (via frameworks like the NIST CSF[20] and sector-specific regulations) and very small businesses (via awareness campaigns and voluntary guidelines). The mid-market occupies a regulatory void that corresponds precisely to its position in the security gap. The CISA Known Exploited Vulnerabilities catalog[21] and similar tools are equally relevant to a $30 million manufacturer and a Fortune 500 company, yet the former has no regulatory mandate to act on them and often lacks the organizational capacity to monitor them.

The SGI data provides an empirical basis for tiered regulatory approaches that impose proportional obligations on mid-market firms, not the full compliance apparatus of enterprise regulation but a minimum standard calibrated to the specific risk profile of the $10M–$50M segment.

5.5. The Compounding Effect

The security gap compounds over time. Firms operating with low DCI scores are less likely to detect breaches early, less likely to contain them effectively, and more likely to experience extended

operational disruption. The 2024 IBM report finds that the average breach lifecycle has shortened to 258 days for the industry overall,[22] but this figure is heavily weighted by enterprises with advanced detection capabilities. For mid-market firms, the effective lifecycle is likely longer, the costs proportionally higher relative to revenue, and the probability of repeat victimization elevated. The security gap, left unaddressed, tends to widen, a finding with significant implications for any longitudinal analysis of mid-market risk.

6. Limitations

This analysis is subject to several material limitations that should inform the reader's interpretation of the findings.

Data granularity. The publicly available data sources used in this analysis do not consistently report metrics at the revenue-band level of granularity required for precise model calibration. The Verizon DBIR and IBM Cost of a Data Breach report segment by organization size, but their categories do not align perfectly with our revenue band definitions. Where interpolation or extrapolation was required, we note this in the methodology. The SGI scores should be understood as structural estimates, not actuarial-grade risk metrics.

Reporting bias. Cybercrime loss data from the FBI IC3 is based on voluntary self-reporting and is widely understood to undercount both incident frequency and total losses. Smaller organizations may be particularly underrepresented, as they are less likely to report incidents and less likely to be captured in industry surveys. This bias potentially understates TEI scores for the lowest revenue bands and overstates the relative position of higher bands.

Cross-industry aggregation. The baseline model uses cross-industry averages for all parameters. In practice, a $30 million healthcare provider faces a materially different threat profile than a $30 million manufacturing firm. The industry sensitivity multiplier in the Target Value Score provides a mechanism for sector-specific adjustment, but the baseline results presented here do not incorporate it. Future iterations of this model should include industry-specific calibrations.

Static snapshot. The model produces a point-in-time estimate based on data from the 2023 to 2024 reporting cycle. The cybersecurity threat landscape is dynamic, and both threat exposure and defensive capability profiles can shift rapidly. The emergence of AI-augmented threats and AI-powered defenses, in particular, may alter the shape of the SGI curve in ways that the current model does not capture.

Proxy variables. Several model inputs rely on proxy variables. Revenue serves as a proxy for organizational complexity, employee count for endpoint density, and industry benchmarks for actual spending. Individual firms may deviate significantly from these proxies. The model characterizes population-level trends, not individual risk profiles.

Normalization artifacts. Min-max normalization to the 0–100 scale is convenient for interpretation but sensitive to the choice of upper and lower bounds. The TEI score of 100 assigned to the $500M+ band is a definitional ceiling, not an empirical observation that this segment faces maximum possible exposure. Changes in the bounding assumptions would shift absolute SGI values, though relative rankings and the location of the SGM would remain stable.

7. Conclusion

This paper has introduced the Security Gap Index as a composite, reproducible metric for estimating the structural cybersecurity deficit facing mid-market businesses. The security gap reaches its maximum in the $25M–$50M revenue band, with an SGR of 2.41, and formalizes an intuition that has circulated among practitioners for years but has not, to our knowledge, been expressed in a quantitative framework grounded in publicly available data.

The implications of this finding extend beyond academic interest. For mid-market executives, the SGI provides an evidence-based framework for understanding their organization's structural risk position and advocating for appropriate resource allocation. For security service providers, the model identifies the segments where marginal investment yields the greatest marginal improvement in defensive posture. For insurers, the non-linear risk profile suggests that current underwriting models may systematically misprice mid-market risk. For regulators, the data supports the case for tiered, proportional cybersecurity requirements that address the specific vulnerabilities of the mid-market without imposing enterprise-scale compliance burdens.

Future research should extend this framework along several axes: longitudinal tracking of SGI scores over time to identify trend directions; industry-specific model calibrations using the sensitivity parameter; integration of the model with breach probability distributions to estimate expected loss functions; and validation against proprietary datasets that may offer more granular firm-level data than currently available public sources. The security gap is real, it is quantifiable, and it is addressable. The first step toward addressing it is understanding where it is widest.

Appendix A: Detailed Component Scores

Table A.1 presents the full decomposition of TEI and DCI component scores across all eight revenue bands.

Band	A	V	F	T	TEI	I	P	M	R	DCI
$1M–$5M	18	25	28	15	22.4	22	5	18	12	18.7
$5M–$10M	32	38	45	34	38.6	28	8	22	14	21.3
$10M–$25M	48	52	62	50	54.2	35	12	28	16	24.8
$25M–$50M	62	65	78	65	67.8	42	15	32	18	28.1
$50M–$100M	74	75	82	72	76.3	55	30	40	28	38.6

Band	A	V	F	T	TEI	I	P	M	R	DCI
$100M–$250M	84	83	86	82	84.1	68	55	58	48	57.2
$250M–$500M	92	90	92	91	91.7	80	72	74	68	74.3
$500M+	100	100	100	100	100.0	92	88	90	85	89.4

Table A.1: Full Component Score Decomposition. A = Attack Surface, V = Target Value, F = Exposure Frequency, T = Third-Party Risk, I = Investment, P = Personnel, M = Technology Maturity, R = IR Readiness. G scores are omitted for space but included in the DCI computation.

Appendix B: Sensitivity Analysis

To assess the robustness of the SGM location, we conducted a sensitivity analysis across three dimensions: component weight perturbation (plus or minus 10% on all weights), spending rate variation (0.50% to 1.00% of revenue), and employee-to-revenue ratio variation (plus or minus 20%). The results are presented in Table A.2.

Scenario	SGM Band	Peak SGI	Peak SGR
Baseline	$25M–$50M	39.7	2.41
Weight perturbation (+10% TEI)	$25M–$50M	42.3	2.58
Weight perturbation (+10% DCI)	$25M–$50M	36.9	2.24
Spending rate = 0.50%	$10M–$25M	34.2	2.52
Spending rate = 1.00%	$25M–$50M	35.1	2.18
Employee ratio +20%	$25M–$50M	41.8	2.53
Employee ratio –20%	$25M–$50M	37.1	2.29
Combined worst case	$10M–$25M	45.6	2.84
Combined best case	$50M–$100M	31.2	1.89

Table A.2: Sensitivity Analysis. SGM Location and Magnitude Under Parameter Variation.

In seven of nine scenarios, the SGM remains located in the $25M–$50M band. Under the reduced spending rate scenario (0.50% of revenue), the SGM shifts leftward to $10M–$25M, reflecting the increased relative severity of underinvestment at lower revenue levels. In the combined best-case scenario, the SGM shifts rightward to $50M–$100M. Across all scenarios, the SGM remains within the $10M–$100M range, and the peak SGR exceeds 1.89, confirming that the structural security deficit in the mid-market is robust to reasonable parameter variation.

Appendix C: Adequate Spend Gap by Revenue Band

Table A.3 quantifies the gap between benchmark security spending and the modeled adequate spend threshold for each revenue band. The Spend Gap column represents the additional annual investment required to achieve a DCI of 60, inclusive of one dedicated security FTE (loaded cost: $120,000).

Revenue Band	Benchmark Spend	Adequate Spend	Spend Gap	Gap as % Rev	Gap / Spend
$1M–$5M	$20,700	$91,250	$70,550	2.35%	3.41x
$5M–$10M	$51,750	$104,500	$52,750	0.70%	1.02x
$10M–$25M	$120,750	$130,750	$10,000	0.06%	0.08x
$25M–$50M	$258,750	$177,500	—	—	—
$50M–$100M	$517,500	$241,250	—	—	—
$100M–$250M	$1.21M	$385,000	—	—	—
$250M–$500M	$2.59M	$610,000	—	—	—
$500M+	$6.90M+	$1.13M+	—	—	—

Table A.3: Benchmark vs. Adequate Cybersecurity Spending by Revenue Band. Where the benchmark exceeds the minimum adequate threshold, the spend gap is not applicable; the adequate spend model excludes advanced tooling and full SOC operations that enterprise-grade defense requires.

References

1. Analysys Mason. (2024). SMB IT Spending Forecast: Driving Business Growth and Increasing Efficiency. Analysys Mason Limited.
2. ConnectWise. (2025). The State of SMB Cybersecurity Report. ConnectWise, Inc.
3. Cybersecurity and Infrastructure Security Agency (CISA). (2025). Known Exploited Vulnerabilities Catalog. U.S. Department of Homeland Security.
4. Federal Bureau of Investigation. (2025). 2024 Internet Crime Report. Internet Crime Complaint Center (IC3).
5. Global Technology Industry Association (GTIA). (2025). SMB Technology and Buying Trends 2025. GTIA.
6. IANS Research and Artico Search. (2024). 2024 Security Budget Benchmark Report. IANS Research.
7. IANS Research and Artico Search. (2025). 2025 Security Budget Benchmark Report. IANS Research.
8. IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation and Ponemon Institute.
9. ISC2. (2024). 2024 Cybersecurity Workforce Study. International Information System Security Certification Consortium.
10. Keepnet Labs. (2025). 2025 Verizon DBIR: Key Facts, Trends and Statistics. Keepnet Labs.
11. National Institute of Standards and Technology. (2024). Cybersecurity Framework 2.0 (NIST CSF 2.0). U.S. Department of Commerce.
12. Netwrix. (2023). 2023 Hybrid Security Trends Report. Netwrix Research Lab.
13. Proofpoint. (2024). 2024 Voice of the CISO Report. Proofpoint, Inc.
14. Vanson Bourne. (2025). SMB Security Research. Cited in ConnectWise State of SMB Cybersecurity Report 2025.
15. Verizon. (2024). 2024 Data Breach Investigations Report (DBIR), 17th Edition. Verizon Business.
16. Verizon. (2025). 2025 Data Breach Investigations Report (DBIR), 18th Edition. Verizon Business.

Disclaimer

affiliated institution. All data sources are publicly available and cited in the footnotes and the references section. Quantitative models are original constructions based on aggregated industry data and are subject to the assumptions and limitations described in Sections 2 and 6. The Security Gap Index (SGI) is a composite metric developed for this analysis and has not been independently validated by external parties. No proprietary data, classified information, or client data was used in the preparation of this report. All data was accessed between November 2025 and February 2026. Reproduction or redistribution of this report, in whole or in part, requires attribution to Bridgham Cyber, LLC and the author. For questions regarding methodology or data, contact headofresearch@bridghamcyber.com.

Vigil publishes quantitative research on cybersecurity economics, threat modeling, and risk analysis. Reports are issued as appropriate in the analyst's judgment and do not follow a fixed publication schedule.