“CYBERCRIME AS A SYSTEMIC BUSINESS RISK: ORGANIZATIONAL EXPOSURE, ECONOMIC CONSEQUENCES, AND A STRATEGIC RESILIENCE FRAMEWORK FOR THE MID-MARKET”

Research Paper

Peter Wilfahrt, Swiss School of Business and Management, Geneva, Switzerland, pw@pw.is

“Abstract”

This paper presents a systematic meta-analysis of major empirical cybercrime studies published between 2020 and 2026. Drawing on evidence from the FBI IC3, Verizon DBIR, IBM Cost of a Data Breach, Bitkom Wirtschaftsschutz, and ENISA Threat Landscape reports, it examines the economic scale of cybercrime, dominant attack vectors, and the persistent gap between organizational exposure and preparedness. Applying Routine Activity Theory, Organizational Resilience Theory, and Institutional Theory, the paper explains why mid-market organizations remain disproportionately vulnerable despite widely available risk information. Key findings include global cybercrime damages reaching USD 9.5 to 12 trillion in 2024, ransomware present in 44% of all confirmed breaches, and German business losses totaling EUR 202.4 billion in 2025. The paper proposes a Risk-Tiered Cyber Resilience Framework (RTCRF) translating empirical evidence into proportionate security investment guidance for mid-market organizations.

Keywords: *cybercrime, organizational resilience, ransomware, data breach, SME security, cyber risk management, threat landscape, routine activity theory, cybercrime economics*

1 Introduction

In 2025, the FBI’s Internet Crime Complaint Center received 1,008,597 complaints from American citizens and businesses, reporting losses of USD 20.9 billion, a 26% increase over the prior year (Federal Bureau of Investigation, 2026). That figure covers one country and only the incidents someone bothered to report. Once industry estimates and unreported cases are added, the annual cost of cybercrime to the global economy already exceeded USD 9.5 trillion in 2024.

Numbers at this scale are hard to grasp. USD 9.5 trillion is roughly equivalent to the combined GDP of Japan, Germany, and the United Kingdom. Unlike conventional crime, cybercrime does not require physical proximity, territorial jurisdiction, or substantial resources. A ransomware campaign that cripples a hospital network can be launched from a laptop in a different hemisphere with tools rented for a few hundred dollars on darknet marketplaces.

This paper is motivated by a specific, practical observation. Despite more than a decade of escalating losses and a growing body of empirical evidence about attack patterns and risk factors, the majority of organizations remain structurally unprepared. Bitkom (2025) found that 87% of German companies were victims of data theft, espionage, or sabotage in the preceding twelve months, yet only half considered themselves well-prepared to handle a cyberattack. Verizon Business (2025) showed that 44% of all analyzed data breaches involved ransomware, a figure that jumps to 88% for small and medium-sized enterprises.

This gap between what is known and what is done is the problem this paper addresses. At its core it is a management problem, and only secondarily a technical one. Organizations misallocate security budgets, underestimate tail risks, and treat cybersecurity as a cost center rather than a risk mitigation function with quantifiable return.

The paper pursues three objectives. First, it synthesizes the most significant empirical evidence from major cybercrime studies into a unified picture of the threat landscape as it stands in 2025 and 2026. Second, it applies Routine Activity Theory and Organizational Resilience Theory to explain why the current patterns of victimization are predictable and structurally reproducible. Third, it proposes a practical framework, the Risk-Tiered Cyber Resilience Framework (RTCRF), to guide mid-market organizations in closing the gap between exposure and preparedness.

1.1 Scope and limitations

This paper focuses on cybercrime as it affects private sector organizations, with particular attention to the mid-market segment (companies with 10 to 500 employees). Nation-state cyber operations are addressed where they intersect with economic harm to businesses, but strategic military or intelligence dimensions are outside this paper's scope. The geographic focus is primarily the United States, the European Union, and Germany, reflecting the availability of high-quality longitudinal data from the FBI, ENISA, and Bitkom respectively.

The paper relies on secondary data synthesized from published studies. The limitations inherent in each source, including underreporting, sampling bias, and varying definitions of 'cybercrime' or 'data breach,' are acknowledged in the methodology section. The proposed RTCRF is conceptual; its empirical validation is recommended as a direction for further research.

2 Problem Statement

Ignorance does not explain why the problem persists. By 2026, threat intelligence is abundant, guidance has been published in volume, and the trajectory of losses is well documented. What is missing is action: organizations, particularly mid-market firms, systematically fail to translate available information into proportionate protective action.

Three empirical observations define the problem. First, the cost of cybercrime to organizations is growing faster than the investments made to prevent it. IBM Security/Ponemon Institute (2024) put the average cost per breach at USD 4.88 million, a 10% increase over 2023 and the largest annual rise since the COVID-19 pandemic. Bitkom (2025) found that German companies spend an average of 18% of their IT budget on security, up from 9% in 2022, yet the total damage in Germany grew by 8% year-on-year to EUR 289.2 billion. Spending is rising; losses are rising faster.

Second, attackers have become structurally more efficient. CrowdStrike (2025) documented an average 'breakout time' of 48 minutes, down from 62 minutes the year before. The fastest observed breakout in 2024 was 51 seconds. AI-assisted attack tooling, available as a service for minimal upfront cost, allows attackers to scale operations that previously required significant human labor. Malicious large language models, including WormGPT and FraudGPT, automate phishing content generation in any language at industrial volume.

Third, the risk is not evenly distributed. Verizon Business (2025) found that ransomware featured in 88% of SMB data breaches, compared with 39% in large enterprises. SMBs are not attacked more often than large firms. Once an intrusion succeeds, however, they are far less able to detect, contain and recover from it. The absence of dedicated security teams, the reliance on unmanaged devices, and the lower investment in detection tooling all compound exposure.

The research problem can be stated precisely: there is a measurable and persistent gap between the organizational risk exposure documented in empirical cybercrime studies and the protective measures organizations actually implement. This gap is widest in mid-market firms, and it is getting wider as attack capabilities scale faster than defenses.

3 Research Questions and Objectives

This paper is organized around four research questions:

RQ1: What does the synthesis of major empirical cybercrime studies reveal about the economic scale, dominant attack vectors, and threat actor profiles of cybercrime between 2020 and 2026?

RQ2: Which theoretical frameworks best explain the persistence of organizational vulnerability to cybercrime despite widely available risk information?

RQ3: What structural characteristics differentiate organizations with high cyber resilience from those with high cyber exposure, as evidenced by the empirical literature?

RQ4: What minimum viable framework enables mid-market organizations to systematically reduce their cybercrime exposure in proportion to their actual risk profile?

The four corresponding objectives are to synthesize the empirical evidence base, to build a theoretically grounded explanation for the observed patterns, to identify the organizational factors that differentiate high-resilience from low-resilience firms, and to translate these findings into a practical management framework.

4 Literature Review

Academic and practitioner research on cybercrime has grown substantially since the mid-2000s. This review is organized into three areas: the economics of cybercrime, theoretical frameworks applied to organizational victimization, and the empirical evidence on organizational resilience.

4.1 The economics of cybercrime

Early attempts to quantify cybercrime losses were plagued by definitional inconsistency and severe underreporting (Anderson et al., 2013). By the early 2010s, Florencio and Herley (2011) had already cautioned against treating self-reported cybercrime loss figures as reliable, noting that survey methodologies systematically overstated costs by extrapolating from small samples of high-loss victims. This methodological critique remains valid today and is why this paper draws primarily on administrative data (Federal Bureau of Investigation, 2026) and large-sample empirical studies (Verizon Business, 2025; IBM Security/Ponemon Institute, 2024) rather than extrapolated survey estimates.

Becker's (1968) rational crime model provides the foundational economic logic: criminal behavior persists when the expected returns exceed the expected costs, adjusted for the probability of detection and sanction. In cybercrime, the structural features of the internet tilt this calculus in favor of attackers. Detection rates are low, successful prosecutions lower still, and the marginal cost of scaling an attack is close to zero once the tooling is built. The emergence of Cybercrime-as-a-Service (CaaS) ecosystems has further reduced the technical barrier to entry.

Levi (2017) introduced the concept of 'harm chains' to map how cyber-enabled fraud inflicts cascading economic damage beyond the immediate loss, including regulatory penalties, reputational harm, and increased insurance premiums. This is consistent with the IBM Security/Ponemon Institute (2024) finding that lost business and post-breach response costs increased by nearly 11% between 2023 and 2024, reaching USD 1.47 million per incident on top of the direct breach cost.

More recent contributions have examined cybercrime as an industry. The World Cybercrime Index (Miranda-Morales et al., 2024) applied a structured survey to cybersecurity experts across multiple countries to identify the primary sources of cybercrime at a national level. Their finding that a small number of countries (Russia, Ukraine, China, the United States, and Nigeria) account for a disproportionate share of cybercriminal activity has implications for threat intelligence and attribution, though the authors caution against treating national origin as a proxy for state direction.

4.2 Theoretical frameworks for organizational victimization

Routine Activity Theory (RAT), originally developed by Cohen and Felson (1979), posits that crime occurs when three conditions converge: a motivated offender, a suitable target, and the absence of a capable guardian. In cybercrime, this convergence is structurally reproduced at scale by the architecture of the internet itself. Target suitability has been operationalized as a function of value, visibility, accessibility, and inertia. Businesses that operate internet-facing services, store sensitive customer data, and run unpatched legacy systems score high on all four dimensions (Holt and Bossler, 2009; Choi, 2008; Pratt et al., 2010).

Organizational Resilience Theory (ORT) examines how organizations absorb, adapt to, and recover from disruptive events (Weick, 1993; Hollnagel et al., 2006; Duchek, 2020). The resilience literature distinguishes between resistance (preventing an attack from succeeding) and recovery (restoring normal operations after a successful attack). The empirical evidence now suggests that investing solely in prevention produces diminishing returns for mid-market firms. A resilience-oriented approach plans for the breach that will eventually happen and measures success by recovery time and loss containment (Björck et al., 2015; Linkov et al., 2019).

Institutional Theory (DiMaggio and Powell, 1983) offers a complementary explanation for why organizations underinvest in cybersecurity despite clear evidence of risk. Mid-market firms often implement cybersecurity measures not because of a rigorous threat assessment but because their industry peers do the same (mimetic isomorphism), because consultants recommend standard controls (normative isomorphism), or because contracts or regulations mandate minimum standards (coercive isomorphism). This compliance-driven approach leads organizations to invest at the minimum required level rather than at the level proportionate to their actual exposure. Compliance also lags the threat: ENISA (2024) found that 11 of the 15 most frequently exploited vulnerability types in 2023 were first exploited as zero-days, before any vendor patch existed.

4.3 Empirical evidence on organizational resilience

IBM Security/Ponemon Institute (2024) provides the most granular empirical evidence on factors that differentiate high-cost from low-cost breach outcomes. Organizations with a tested incident response team and plan incurred an average breach cost of USD 3.26 million, compared with USD 5.29 million for organizations without these capabilities, a 58% reduction. Extensive use of security AI and automation reduced breach costs by an average of USD 2.2 million per incident, the single largest cost-reduction factor in the study.

Verizon Business (2025) found that multi-factor authentication (MFA) was absent in the vast majority of identity-based intrusions, consistent with Microsoft (2025) telemetry data showing MFA prevents more than 99% of automated identity attacks. Bitkom (2025) provides evidence specific to the German mid-market: organizations investing more than 20% of their IT budget in security reported lower rates of successful attacks, yet more than half of surveyed companies still fell below this threshold in 2025.

5 Theoretical Framework

This paper integrates Routine Activity Theory and Organizational Resilience Theory into a unified explanatory framework used to derive the practical components of the RTCRF. RAT explains the supply side of cybercrime victimization: why certain organizations are attacked and why the volume of attacks has grown so rapidly. The digital economy has increased target suitability, reduced the cost of motivated offending through CaaS ecosystems, and systematically degraded guardian capability in the mid-market through resource constraints and skills gaps.

ORT explains the demand side: what organizations can do to reduce their expected loss even when attacks succeed. The integration of RAT and ORT generates a specific prediction: the expected economic loss from cybercrime is a function of target suitability multiplied by recovery capability. Organizations with high target suitability can substantially reduce expected loss by investing in recovery

capability. Conversely, organizations that invest only in perimeter defense remain highly vulnerable to novel attack vectors.

Institutional Theory explains why the observed underinvestment persists. Organizations respond to institutional signals (compliance requirements, industry benchmarks, audit standards) rather than to actuarial risk. Until institutional signals align with actual exposure levels, there will be a systematic gap between what organizations do and what would be economically rational given their risk profile.

6 Research Methodology

6.1 Research design

This paper employs a systematic meta-analysis design, integrating quantitative evidence from multiple published primary studies. Meta-analysis is appropriate here because the research questions concern patterns across studies rather than findings from a single dataset. The approach follows the systematic review methodology outlined by Kitchenham and Charters (2007), adapted for management research. The study is positioned within a post-positivist epistemological tradition: the cybercrime phenomenon has an objective existence and produces measurable economic effects, but our ability to measure it is constrained by reporting biases, definitional variation, and the inherently opaque nature of criminal activity.

6.2 Data sources and selection criteria

Primary data sources were selected according to three criteria: methodological transparency, sample size sufficient to support cross-sector or cross-national inference, and temporal coverage extending into 2024 or 2025. Table 1 summarizes the ten primary sources included in the analysis.

Source	Publisher	Data basis	Year(s)	Geography
2025 Internet Crime Report	FBI / IC3	1,008,597 victim complaints	2020-2025	USA/Global
Data Breach Investigations Report (DBIR)	Verizon Business	22,052 incidents; 12,195 breaches	2020-2025	139 countries
Cost of a Data Breach	IBM Security/Ponemon Inst.	604 organizations, 17 industries	2020-2025	Global
Wirtschaftsschutz	Bitkom e.V.	>1,000 companies, representative	2021-2025	Germany
ENISA Threat Landscape	ENISA	11,079 incidents (2024 edition)	2022-2025	EU/Europe
Global Cybersecurity Outlook	World Economic Forum	Executive survey	2024-2025	Global
Crypto Crime Report	Chainalysis	Blockchain transaction analysis	2024-2025	Global

Source	Publisher	Data basis	Year(s)	Geography
Cybersecurity Almanac	Cybersecurity Ventures	Aggregation >200 studies	2025	Global
Digital Defense Report	Microsoft	Proprietary telemetry data	2024-2025	Global
Global Threat Report	CrowdStrike	Telemetry, 250+ threat groups	2025	Global

Table 1. Primary data sources included in meta-analysis.

6.3 Analytical approach and limitations

The analysis proceeds in three stages. The first stage maps each primary source against the four research questions. The second stage applies thematic synthesis (Thomas and Harden, 2008), grouping findings into common themes across sources to identify convergent and divergent evidence. The third stage applies the theoretical framework to generate the practical RTCRF. Where sources provide conflicting estimates, the range is reported and methodological reasons for divergence are explained.

Three limitations are material. First, underreporting is pervasive: FBI IC3 data reflects only incidents reported to that channel, and Verizon DBIR covers only incidents processed through contributing partners. Second, studies use different definitions of key terms. Third, the proposed RTCRF is conceptual and has not been empirically validated in a prospective study. Validation through field research is a direction for future work.

7 Findings

7.1 The scale and trajectory of cybercrime losses (RQ1)

The ten-source synthesis produces a consistent picture of accelerating losses. Global cybercrime damages reached an estimated USD 9.5 to 12 trillion in 2024. Statista (2025) projects USD 15.6 trillion by 2029. Cybersecurity Ventures (2025) projects USD 10.5 trillion annually by 2025 and a ransomware-specific trajectory reaching USD 265 billion per year by 2031.

FBI IC3 data show that reported losses in the United States grew from USD 4.1 billion in 2020 to USD 20.9 billion in 2025, a compound annual growth rate of roughly 38% (Federal Bureau of Investigation, 2026). IBM Security/Ponemon Institute data show average breach costs rising from USD 3.86 million in 2020 to USD 4.88 million in 2024, before falling to USD 4.44 million in 2025 (IBM Security/Ponemon Institute, 2025), the first decline the report attributes to AI-assisted detection and containment.

In Germany, Bitkom's longitudinal data (2024; 2025) show the same trend. Cybercrime-attributable losses grew from EUR 148.2 billion in 2023 to EUR 202.4 billion in 2025, a 37% increase over two years. Cybercrime now accounts for 70% of total economic damage from data theft, espionage, and sabotage. The share of German companies reporting at least one incident rose from 72% in 2023 to 87% in 2025.

7.2 Attack vectors and threat actor profiles (RQ2)

Verizon Business (2025) found that stolen credentials were the most common initial access vector at 22% of breaches. Vulnerability exploitation reached 20%, a 34% increase over the prior year, driven by

a sharp rise in zero-day exploitation of edge devices and VPN appliances. Of the 15 most frequently exploited vulnerability types in 2023, 11 were first exploited as zero-days (ENISA, 2024). The median time to full remediation was 32 days, and 46% of vulnerabilities in the monitored dataset were never fully patched.

Ransomware was present in 44% of confirmed breaches, up from 32% the prior year (Verizon Business, 2025), rising to 88% for SMB breaches. The median ransom payment was USD 115,000, but 64% of victim organizations refused to pay. Chainalysis (2025) recorded the same shift in blockchain data: total ransomware payments fell by roughly 35% in 2024 to about USD 814 million, the first annual decline since 2022. Third-party involvement in breaches doubled year-over-year, reaching 30% of all analyzed breaches, consistent with Gartner's (2022) projection that 45% of organizations globally would experience a software supply chain attack by 2025.

Miranda-Morales et al. (2024) identified Russia, Ukraine, China, the USA, and Nigeria as the primary national sources of cybercriminal activity. Russian-language actors dominate the ransomware ecosystem, accounting for an estimated 75% of ransomware revenue flows (Global Initiative Against Transnational Organized Crime, 2025). Verizon Business (2025) documented a 163% increase in espionage-motivated breaches, now accounting for 17% of all incidents. Bitkom (2025) found that 46% of German companies traced at least one attack to Russia and an equal proportion to China.

7.3 Organizational resilience factors (RQ3)

IBM Security/Ponemon Institute (2024) found that organizations with a tested IR team and plan incurred average breach costs of USD 3.26 million versus USD 5.29 million for those without, a 58% reduction. Extensive use of security AI and automation reduced costs by USD 2.2 million per incident. Microsoft (2025) telemetry data show that MFA prevents more than 99% of automated identity-based attacks. SpyCloud (2025) research shows that 46% of compromised business credentials originated from unmanaged personal devices on which infostealer malware had executed without detection.

The World Economic Forum (2025) found that 72% of organizational leaders reported increased cyber risks, yet a significant share lacked a formal, tested incident response plan. Awareness of the risk has outpaced governance of it. The ENISA (2025) finding that 80% of phishing emails in early 2025 used AI in some form adds a second problem: detection heuristics built for human-written phishing are losing their value.

7.4 The AI amplification effect (RQ4)

AI is changing both sides of the cybercrime equation, but not at the same pace. On the offensive side, ENISA's (2025) finding that over 80% of phishing emails use AI in some form shows how little effort it now takes to produce convincing, personalized lures at scale. Deepfakes are used in voice phishing and CEO fraud, with iProov (2025) documenting a surge in face-swap attacks and identity-spoofing operations throughout 2024.

On the defensive side, IBM Security/Ponemon Institute's (2024) observation of a USD 2.2 million average cost reduction from AI security automation is material. But adoption of AI-powered defenses is uneven: large organizations with dedicated security teams adopt new tooling faster than SMBs. The net effect is a widening capability gap between well-resourced organizations and the mid-market.

8 The Risk-Tiered Cyber Resilience Framework (RTCRF)

The Risk-Tiered Cyber Resilience Framework turns the empirical findings and the theoretical framework into guidance that mid-market organizations can act on. It is built on three premises: no organization can prevent all successful cyberattacks, so the framework measures both prevention and recovery; the optimal security investment level is proportionate to risk exposure, not to peer benchmarks or compliance requirements; and a small number of high-impact controls account for the majority of empirically demonstrated loss reduction.

8.1 Risk tier assignment

Organizations are assigned to one of three risk tiers based on four input dimensions: sector (using known sector-specific attack frequency data from FBI, Verizon Business, and ENISA), data sensitivity (the volume and sensitivity of personal, financial, and operational data held), attack surface (the extent of internet-facing systems, remote access, and third-party integrations), and prior incident history. Table 2 defines each tier.

Tier	Risk profile	Representative examples	Base investment floor
Tier 1: Standard	Low data sensitivity, limited internet exposure, low-value sector	Local service businesses, small retail, simple B2C operations	15% of IT budget
Tier 2: Elevated	Moderate data sensitivity or supply chain exposure, regulated sector	Mid-market manufacturing, professional services, healthcare	20-25% of IT budget
Tier 3: Critical	High data sensitivity, significant IP, critical infrastructure role	Financial services, defense supply chain, utilities, pharma	25-35% of IT budget

Table 2. RTCRF risk tier definitions. Investment floors calibrated to Bitkom (2025) survey data.

8.2 Minimum viable protection layer

Across all three tiers, five controls have the highest empirical evidence for loss reduction and form the Minimum Viable Protection Layer (MVPL): (1) Multi-factor authentication on all external-facing systems and privileged accounts, which Microsoft (2025) confirms blocks more than 99% of automated credential-based intrusion attempts; (2) Offline, tested backups addressing the primary leverage mechanism of ransomware; (3) Endpoint detection and response (EDR) tooling on all managed devices to reduce lateral movement; (4) Patch management with a maximum 30-day remediation cycle for critical and high vulnerabilities; (5) A tested incident response plan, which IBM Security/Ponemon Institute (2024) associates with a USD 2.03 million reduction in average breach cost.

8.3 Tier-specific extensions and governance integration

Beyond the MVPL, Tier 2 organizations should add network segmentation, third-party risk assessment for key suppliers, and security awareness training with simulated phishing. Tier 3 organizations should additionally implement a Security Operations Center function (internal or managed), threat intelligence integration, privileged access management (PAM), and Zero Trust network architecture. The Zero Trust model was adopted in full or in part by 81% of organizations in the World Economic Forum (2025) survey.

The RTCRF requires board-level reporting of cybersecurity KPIs: time to detect a breach (below 30 days for Tier 1, 14 days for Tier 2, 7 days for Tier 3), time to contain, percentage of critical vulnerabilities patched within SLA, and backup test success rate. These metrics put technical performance into terms a board can act on.

9 Discussion

The synthesis of evidence across ten major studies produces a consistent and uncomfortable picture. The rise in cybercrime losses, from USD 3 trillion in 2015 to an estimated USD 15.6 trillion by 2029, cannot

be blamed on a lack of awareness. The data is public, the guidance is available, and the consequences of underinvestment are visible across every sector. The problem is that institutional and behavioral factors systematically pull organizational decision-making away from what the actuarial evidence would recommend.

Three dynamics stand out. The first is the SME resilience gap. Verizon Business's (2025) finding that ransomware features in 88% of SMB breaches but only 39% of large enterprise breaches has structural causes. SMBs cannot afford dedicated security teams, cannot sustain the procurement cycles for enterprise security tooling, and do not have the legal and PR resources to manage a major breach. Chambers of commerce, sector associations, and national cybersecurity agencies have a role in addressing this through collective defense models and shared services.

The second dynamic is the speed asymmetry between attackers and defenders. The 48-minute average breakout time documented by CrowdStrike (2025) means that, in a standard SMB environment without active monitoring, an attacker has effectively unlimited time to establish persistence. The response to this asymmetry is automated detection and isolation capability. For mid-market organizations that cannot afford 24/7 human monitoring, managed detection and response (MDR) services are the most affordable route to it.

The third dynamic is AI amplification. ENISA's (2025) finding that 80% of phishing emails now use AI means that an employee can no longer be expected to spot a lure by its clumsy wording. Security awareness training has to change its curriculum faster than it has in the past, and technical controls have to compensate for the reduced reliability of human detection.

10 Practical Implications

For organizational leaders, the most immediate implication is that cybersecurity belongs in risk governance and cannot be left to the IT department alone. IBM Security/Ponemon Institute (2024) shows that organizations with board-level cybersecurity oversight incur lower breach costs. This means regular board reporting of security KPIs, defined risk appetite statements for cyber exposure, and a named executive with accountability for the security program.

For boards of directors, the primary implication is accountability for the risk tier assessment. Bitkom's (2025) finding that 59% of German companies consider cyberattacks existentially threatening suggests that boards have some awareness of the risk; the question is whether that awareness translates into governance that closes the investment gap. Organizations that have not yet implemented MFA universally, tested their backup infrastructure, and prepared an incident response plan should not be investing in advanced threat intelligence platforms.

For policymakers, the evidence supports the case for minimum security standards calibrated to sector and data sensitivity, rather than uniform compliance requirements. The NIS2 Directive in the European Union is a step in this direction; the challenge is ensuring that enforcement mechanisms are proportionate and that compliance does not become an end in itself. For the research community, the primary gap is the absence of prospective, longitudinal studies measuring the actual impact of specific security investments on breach frequency and cost in the mid-market segment.

11 Conclusion

Cybercrime is the largest property crime problem in human history, and it is growing. The evidence assembled in this paper leaves little doubt about the direction of the trend: losses are rising faster than defenses, attacks are becoming cheaper to launch, and the mid-market is bearing the largest proportional share of the damage.

The theoretical synthesis offered here, combining Routine Activity Theory's explanation of victimization patterns with Organizational Resilience Theory's framework for preparedness, and

Institutional Theory's account of why rational underinvestment persists, explains both the problem's persistence and its tractability. The problem persists because institutional pressures push organizations toward compliance rather than proportionate risk management. It is tractable because the empirical evidence identifies a small set of high-return controls that reduce expected losses at costs most organizations can afford.

The Risk-Tiered Cyber Resilience Framework proposed here is a prioritization tool built on what the evidence says works. Its claim is straightforward: organizations that implement the Minimum Viable Protection Layer for their risk tier, integrate security into board governance, and measure resilience outcomes rather than only prevention outcomes will incur substantially lower losses. That claim is testable, and testing it is the most productive direction for future research.

Inaction is itself a decision. An organization that runs without MFA, with untested backups and without an incident response plan has already chosen how much risk it accepts, even if nobody in the boardroom would put it that way. With attackers moving from initial access to lateral movement in 48 minutes on average, the more useful question for such an organization is how long it would take to notice.

References

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M., Levi, M., Moore, T. and Savage, S. (2013) 'Measuring the cost of cybercrime', in Böhme, R. (ed.) *The economics of information security and privacy*. Berlin: Springer, pp. 265-300.

Becker, G.S. (1968) 'Crime and punishment: An economic approach', *Journal of Political Economy, 76*(2), pp. 169-217.

Bitkom e.V. (2024) *Wirtschaftsschutz 2024* [Online]. Bitkom Research. Available at: https://www.bitkom.org (Accessed: 21 September 2026)

Bitkom e.V. (2025) *Wirtschaftsschutz 2025* [Online]. Bitkom Research. Available at: https://www.bitkom.org (Accessed: 21 September 2026)

Björck, F., Henkel, M., Stirna, J. and Zdravkovic, J. (2015) 'Cyber resilience: Fundamentals for a definition', in Rocha, A. et al. (eds.) *New contributions in information systems and technologies* (AISC, Vol. 353). Cham: Springer, pp. 311-316.

Chainalysis (2025) *2025 crypto crime report.* Chainalysis Inc.

Choi, K.S. (2008) 'Computer crime victimization and integrated theory', *International Journal of Cyber Criminology, 2*(1), pp. 308-333.

Cohen, L.E. and Felson, M. (1979) 'Social change and crime rate trends: A routine activity approach', *American Sociological Review, 44*(4), pp. 588-608.

CrowdStrike (2025) *2025 global threat report.* CrowdStrike Holdings.

Cybersecurity Ventures (2025) *2025 cybersecurity almanac.* Cybersecurity Ventures.

DiMaggio, P.J. and Powell, W.W. (1983) 'The iron cage revisited', *American Sociological Review, 48*(2), pp. 147-160.

Duchek, S. (2020) 'Organizational resilience: A capability-based conceptualization', *Business Research, 13,* pp. 215-246.

ENISA (2024) *ENISA threat landscape 2024* [Online]. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu (Accessed: 21 September 2026)

ENISA (2025) *ENISA threat landscape 2025* [Online]. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu (Accessed: 21 September 2026)

Federal Bureau of Investigation (2026) 2025 *internet crime report* [Online]. Internet Crime Complaint Center. Available at: https://www.ic3.gov (Accessed: 21 September 2026)

Florencio, D. and Herley, C. (2011) 'Sex, lies and cybercrime surveys', in *Proceedings of the 10th Workshop on the Economics of Information Security (WEIS 2011).* Fairfax, VA: George Mason University.

Gartner (2022) *Predicts 2022: Supply chain security.* Gartner Research.

Global Initiative Against Transnational Organized Crime (2025) *Cybercrime and criminal networks: 2025 global assessment* [Online]. GI-TOC. Available at: https://globalinitiative.net (Accessed: 21 September 2026)

Hollnagel, E., Woods, D.D. and Leveson, N. (eds.) (2006) *Resilience engineering: Concepts and precepts*. Aldershot: Ashgate.

Holt, T.J. and Bossler, A.M. (2009) 'Examining the applicability of lifestyle-routine activities theory', *Deviant Behavior, 30*(1), pp. 1-25.

IBM Security/Ponemon Institute (2024) *Cost of a data breach report 2024* [Online]. IBM Corporation. Available at: https://www.ibm.com/security (Accessed: 21 September 2026)

IBM Security/Ponemon Institute (2025) *Cost of a data breach report 2025* [Online]. IBM Corporation. Available at: https://www.ibm.com/security (Accessed: 21 September 2026)

iProov (2025) *Threat intelligence report 2025: Remote identity under attack* [Online]. iProov Ltd. Available at: https://www.iproov.com (Accessed: 21 September 2026)

Kitchenham, B. and Charters, S. (2007) *Guidelines for performing systematic literature reviews in software engineering*. Technical Report EBSE-2007-01. Keele: Keele University.

Levi, M. (2017) 'Assessing the trends, scale and nature of economic cybercrimes', *Crime, Law and Social Change, 67*(1), pp. 3-20.

Linkov, I. et al. (2019) *Cyber resilience as a new source of value for cyber risk.* Cham: Springer.
Microsoft (2025) *Microsoft digital defense report 2025* [Online]. Microsoft Corporation. Available at: https://www.microsoft.com/security (Accessed: 21 September 2026)
Miranda-Morales, J., Bouchard, M., Shortland, N., Wainwright, L., Leukfeldt, E.R. and Hutchings, A. (2024) 'Mapping the global geography of cybercrime', *PLOS ONE*, 19(4), e0297312. Available at: https://doi.org/10.1371/journal.pone.0297312 (Accessed: 21 September 2026)
Pratt, T.C., Holtfreter, K. and Reisig, M.D. (2010) 'Routine online activity and internet fraud targeting', *Journal of Research in Crime and Delinquency, 47*(3), pp. 267-296.
SpyCloud (2025) *2025 annual identity exposure report* [Online]. SpyCloud Inc. Available at: https://spycloud.com (Accessed: 21 September 2026)
Statista (2025) *Cybercrime damage costs worldwide 2015-2029* [Online]. Statista GmbH. Available at: https://www.statista.com (Accessed: 21 September 2026)
Thomas, J. and Harden, A. (2008) 'Methods for the thematic synthesis of qualitative research in systematic reviews', *BMC Medical Research Methodology, 8,* Article 45.
Verizon Business (2025) *2025 data breach investigations report* [Online]. Verizon Communications. Available at: https://www.verizon.com/dbir (Accessed: 21 September 2026)
Weick, K.E. (1993) 'The collapse of sensemaking in organizations', *Administrative Science Quarterly, 38*(4), pp. 628-652.
World Economic Forum (2025) *Global cybersecurity outlook 2025* [Online]. World Economic Forum. Available at: https://www.weforum.org (Accessed: 21 September 2026)