“BEHAVIOURAL THREATS TO SME WEBSHOPS UNDER EU LAW”

Research Paper

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

”Abstract”

Underground identity markets occupy one end of the cybercrime supply chain. At the other end, in sectors far removed from dark web forums, small webshop operators face a structurally related problem: customers who exploit contractual constructs, liberal return policies, and EU consumer law to systematically extract value without breaking any laws. This paper looks at that threat and argues that it follows the same economic logic as technical cybercrime. Drawing on Routine Activity Theory and Situation Awareness Theory, it develops a seven-type taxonomy of behavioural threats to EU-based SME webshops, constructs a cost impact model calibrated to micro-business scale, and maps the legal and operational countermeasures available under Directive 2011/83/EU and evolving ECJ jurisprudence. Behavioural threats work differently from technical threats, need a different analytical framework, and hardly appear in the research and guidance that European SME operators rely on today. A small number of abusive customers, often as few as two to five per hundred, can eliminate the net margin of an entire customer segment. Cheap improvements in guardianship reduce this exposure considerably.

Keywords: *behavioural threats, SME, e-commerce, serial returning, return fraud, EU withdrawal right, Directive 2011/83/EU, bot traffic, consumer law, routine activity theory*

1 Introduction

Online retail carries a large part of the European economy. By 2024, approximately 140,000 businesses operated in the German B2C e-commerce market alone, and for every euro the sector contributed directly, it stimulated an additional 1.60 euros of economic activity in the broader economy (bevh and Oxford Economics, 2025). Small and medium-sized enterprises make up most of this market. They outnumber large retailers by orders of magnitude, serve local and regional markets with products that platform giants do not, and represent the majority of first-time e-commerce entrants. They are also easier to exploit than the large operators that get most of the academic and policy attention.

The dominant frame in cybersecurity research treats threats to e-commerce businesses as technical problems: server vulnerabilities, credential theft, denial-of-service attacks, malware infection. That frame captures something real. German SMEs face genuine technical risks, with over 57% of firms employing 50 to 250 people reporting cyberattacks in the three years preceding the HDI Cyber Study (HDI Versicherung and Sirius Campus, 2022), at an average cost of EUR 95,000 per successful incident. But the frame hides a different class of threats. They never show up in intrusion detection logs, they need no hacking skills, and no firewall stops them, because they run through legitimate system functions such as consumer rights law and the merchant's own return portal.

This paper calls this class behavioural threats: actions by customers or automated agents that systematically extract value from an e-commerce operator by exploiting legal entitlements, policy tolerances, or informational asymmetries, without constituting illegal system access. The category includes serial returning, wardrobing, bracketing, friendly fraud, organised seller sabotage, and bot-

driven inventory manipulation. None of these are new. What is missing is a systematic academic treatment of them as one category in the SME context, and almost any analysis that takes the EU legal framework into account.

That legal framework matters more than the US-centric literature suggests. The right of withdrawal codified in Directive 2011/83/EU, implemented in Germany as Sections 355 and 312g of the Civil Code (BGB), gives consumers a 14-day no-questions-asked cancellation right for all distance contracts. There is no statutory equivalent in US or UK consumer law, where return policies are matters of commercial discretion. The directive thus gives abusive customers a legal backstop that merchants elsewhere never have to deal with, yet most published research on return fraud uses US or UK datasets.

This paper addresses four research questions. First, what distinct categories of behavioural threat affect EU-based SME webshop operators, and how do they differ structurally from technical threats? Second, how does the cost burden of these threats differ between micro-businesses and large retailers? Third, what legal countermeasures are available to EU merchants under the withdrawal right framework, including through evolving ECJ and BGH jurisprudence? Fourth, which prevention measures offer a positive return on investment for operators with limited resources?

1.1 Significance of the study

A systematic review of 1,090 SME cybersecurity studies published between 2017 and 2024 found that the field keeps confirming early findings without producing new ones, that behavioural threats do not appear in the literature at all, and that the EU regulatory context is almost entirely unaddressed (Rombaldom, Becker and Johnson, 2024). Chambers of commerce, industry associations, and digital advisory bodies across Europe currently advise member businesses on cybersecurity risks on the basis of evidence that says nothing about the threats most likely to erode the margins of a small webshop over the course of a normal trading year.

2 Literature Review

2.1 SME cybersecurity: state of the field

Research on cybersecurity in small and medium-sized enterprises has grown substantially since the mid-2010s, but the field has clear limits. The systematic review by Rombaldom, Becker and Johnson (2024), covering 132 papers from 2017 to 2024, found the same pattern again and again. Studies cluster around a few themes, mainly awareness gaps, resource constraints, technical vulnerabilities, and regulatory compliance, and use methods, samples, and geographic contexts that limit generalisability to European operators.

The perception problem is well documented: SMEs underestimate their exposure to attack. The Sectigo State of Website Security Report (2021), surveying 1,167 SME decision-makers, found that 48% believed they were too small to be targeted despite 50% having already experienced a website attack and 40% reporting monthly attacks. The Resource-Based View of cybersecurity, tested empirically with 239 UK SMEs by Tantithamthavorn, Jiarpakdee and Croft (2023), found that cybersecurity incidents were a stronger driver of resilience than cybersecurity capabilities, which suggests that operators who have never suffered a loss from behavioural abuse are at a disadvantage.

The EU regulatory context is almost entirely absent from the SME cybersecurity literature. Studies reference GDPR compliance as a challenge, but the specific implications of the Consumer Rights Directive for merchant exposure to return abuse, or the evolving ECJ case law on withdrawal right misuse, appear in none of the reviewed papers. This gap is the main reason for the present research.

2.2 Return fraud and behavioural abuse research

Research on return fraud skews heavily toward North American contexts and large-retailer samples. The NRF and Appriss Retail 2024 Consumer Returns report estimated total US retail returns at USD 685

billion, representing 13.21% of retail sales, with fraud and abuse accounting for 15.14% of total returns, approximately USD 103 billion. The 2025 NRF and Happy Returns report projected USD 849.9 billion in total returns at a 15.8% rate, with 9% of returns classified as fraudulent. These figures show the scale of the problem but say nothing about operators with revenues in the tens or hundreds of thousands of euros.

Merlano et al. (2024), in the International Journal of Physical Distribution and Logistics Management, surveyed 485 UK consumers to evaluate the effectiveness of retailer counter-fraud interventions. Using the fraud triangle and the theory of planned behaviour, they found that consumers judge interventions by fairness as much as by deterrence. Measures seen as disproportionate met resistance even among honest shoppers. For small operators lacking the brand equity of large retailers, aggressive deterrence may cost more in customer attrition than it saves in fraud prevention. The ECR Loss report (Beck, 2024/2025) documented the professionalisation of Refund-as-a-Service operations, in which specialist fraud intermediaries execute returns fraud on behalf of clients for a fee, a development consistent with RAT predictions about offender displacement as large retailers improve their detection capabilities.

2.3 Bot traffic: research and impact

The Thales Bad Bot Report (2026) puts automated traffic at 53% of global web traffic in 2025, with 40% classified as malicious. Geographic traffic anomalies are a problem of their own. According to DreamHost and Imperva analysis (2025), Ireland generates 40.7% of daily bot traffic by visit share and Singapore 13%, concentrations driven by major cloud provider data centres rather than by purchase intent. For a small webshop serving exclusively the DACH region, traffic from these origins consists of automated agents rather than customers, and it costs real money in bandwidth and distorts analytics.

2.4 EU consumer law: the withdrawal right

Directive 2011/83/EU on Consumer Rights grants consumers a minimum 14-day right of withdrawal from all distance contracts without requirement to state a reason. The directive has been amended three times since 2014 and remains the governing framework for physical goods sold online. The statutory exceptions in Article 16 and Section 312g(2) BGB cover perishable goods, personalised products, sealed hygiene items, and digital content after delivery commencement. For most goods sold by small webshops, none of these exceptions apply.

The most important recent legal development is ECJ Case C-97/22 (May 2023). The court held that the withdrawal right serves consumer protection rather than unjust enrichment and that demonstrably abusive exercises may be denied legal effect (Laukemann, 2025). The BGH additionally restricted the eternal withdrawal right in 2024, ruling that a right exercised on the basis of a minor formal defect many years after contract conclusion may constitute an abuse of rights under Section 242 BGB. For the first time, merchants have a European-level mechanism for merchant resistance to systematic return abuse, provided the merchant can document specific circumstances suggesting misuse.

3 Theoretical Framework

3.1 Routine activity theory

Routine Activity Theory (RAT), developed by Cohen and Felson (1979), posits that predatory acts require three converging elements: a motivated offender, a suitable target, and the absence of capable guardianship. Pratt, Holtfreter and Reisig (2010) extended the theory to online contexts, demonstrating that routine online activities predicted internet fraud victimisation in a survey of 1,206 Virginia households. Johnson and Nikolovska (2022) used COVID-19 lockdowns as a natural experiment and confirmed that online fraud rose as online activity increased and mobility declined, consistent with RAT predictions.

Applied at the operator level, the motivated offender is the serial returner or organised fraud operation, the suitable target is the SME webshop with liberal return policy and no customer-level tracking, and

the absent guardian is the combination of data capacity, analytical tooling, and management attention that large retailers possess. This explains the asymmetry. Large platforms with algorithmic pattern recognition have capable guardianship, small operators do not. RAT also predicts that as guardianship increases for large targets, motivated offenders redirect toward targets with lower guardianship, which fits the documented professionalisation of return fraud aimed at smaller merchants.

3.2 Situation awareness theory

Endsley's (1995) Situation Awareness Theory identifies three sequential cognitive stages: perception of relevant elements, comprehension of their significance, and projection of future states. Applied to SME cybersecurity in a survey of 361 UK firms, Rajapaksa et al. (2024, cited in Rombaldom, Becker and Johnson, 2024) found that both situational awareness and resource availability independently predicted adoption of cybersecurity measures. For behavioural threats, the first failure is perception. An operator who does not track return rates per customer account cannot see that five customers cause most of the loss. The second is comprehension. Even when anomalies show up in aggregate statistics, operators without reference data cannot tell whether the numbers are a problem. The third is projection. Without a model of how the threat develops, operators cannot anticipate escalation or choose when to intervene. SAT therefore points to better information architecture as the main requirement, well before expensive tooling.

3.3 Research model

RAT explains the structural conditions under which behavioural threats emerge and persist. SAT explains why motivated operators fail to detect and respond effectively. Together they generate three testable propositions: (a) SME operators with lower guardianship capacity experience higher rates of behavioural threat incidence; (b) operators with lower situation awareness respond less effectively when incidents occur; and (c) low-cost guardianship enhancements have a higher marginal deterrence value for SMEs than for large retailers because they shift the operator out of the high-vulnerability category in the offender's opportunity assessment. These propositions are offered as hypotheses for the empirical phase of this DBA research programme.

4 Research Methodology

This research adopts an interpretivist philosophical stance, in line with the DBA orientation toward findings practitioners can use. The research design combines a systematic literature review, a doctrinal legal analysis, and a modelled cost impact assessment.

The systematic literature review followed the PRISMA framework across five databases: Business Source Complete, Web of Science, Scopus, SSRN, and Google Scholar. Search terms were developed across three conceptual domains: SME cybersecurity, behavioural threats, and EU legal context. The final search was conducted in March 2026 and yielded 87 sources after deduplication and relevance screening. The doctrinal legal analysis reviewed Directive 2011/83/EU and its amending directives, Regulation 2018/302 (Geoblocking), the GDPR, and the German BGB implementing provisions. ECJ Case C-97/22 and the BGH 2024 withdrawal right ruling were reviewed for applicability to physical goods return abuse. The cost impact assessment used modelled scenarios calibrated to micro-business scale from industry datasets, meant to show the order of magnitude rather than exact figures.

4.1 Limitations

Three limitations should be noted. First, empirical data underpinning the cost model derives primarily from large US retailer samples, requiring extrapolation to European micro-businesses. Second, the legal analysis reflects EU consumer law as of April 2026, an actively evolving framework. Third, this paper does not include primary empirical data from SME operators. Semi-structured interviews with German

and Austrian SME webshop operators, recruited through chamber of commerce networks, are planned as the empirical phase of this DBA research.

5 Findings and Discussion

5.1 A taxonomy of behavioural threats

The literature review and threat analysis produce seven categories of behavioural threat that differ in mechanism, legality, detectability, and impact. Table 1 gives the overview.

Threat type	Legality	Detectability	SME burden
Serial Returning	Legal	Low without tracking	Very high
Wardrobing	Legal	Difficult	High
Bracketing	Legal	Medium	Medium-high
Friendly Fraud	Illegal	Medium	Very high
Seller Sabotage	Grey zone	Very difficult	High
Inventory Hoarding Bots	Illegal	Technically measurable	Medium
Scraper Bots	Grey zone	Technically measurable	Medium

Table 1. Classification of behavioural threat types by legality, detectability, and SME burden

5.2 Serial returning and bracketing

Serial returning describes the habitual purchase of goods with the predominant intention of returning them. The ZigZag and Retail Economics (2024) UK returns benchmark found that 11% of online shoppers qualify as serial returners by behavioural criteria. The NRF and Happy Returns (2025) survey found that 51% of Gen Z consumers acknowledged bracketing, ordering multiple variants to retain one and return the rest, as a routine practice. What makes this a threat is concentration. Redo (2026) found that 2% to 5% of accounts generate a disproportionate share of return-related losses. In Germany, 87% of the top 100 online shops offered free returns in 2023 (ParcelLab and Statista, 2023), which rewards the behaviour.

5.3 Wardrobing

Wardrobing involves purchasing goods for temporary use with the pre-formed intention of return. The fashion sector accounts for 68% of all German online returns (Sendcloud, 2024). The NRF and Appriss Retail (2023) survey found that 49% of retailers reported wardrobing incidents. The operator has a right to claim diminished value under Section 357(7) BGB if consumer use exceeded what is necessary to establish the nature of the goods, but this claim requires condition documentation that most small operators do not maintain.

5.4 Friendly fraud and chargebacks

Friendly fraud occurs when a consumer falsely claims goods were not received or were defective to secure a refund while retaining them. Chargebacks911 (2024) estimated that friendly fraud accounts for

60% to 80% of all chargebacks. Mastercard (2024) estimated total chargeback costs to merchants at USD 117.47 billion in 2023. On a product with 40% gross margin and EUR 80 retail price, a single successful friendly fraud incident generates a total loss of approximately EUR 100 plus chargeback fees, against a foregone margin of approximately EUR 32. The MRC Global eCommerce Payments and Fraud Report (2024) found that European merchants made far less use of compelling evidence procedures to contest chargebacks compared to North American merchants.

5.5 Seller sabotage, bots, and geographic traffic

Seller sabotage means that a competitor purchases large inventory volumes within the return window and returns the entire purchase at the deadline, disrupting availability and imposing processing costs without any net financial loss to the attacker. Bot-driven manipulation covers hoarding bots that populate carts without completing purchases, scraper bots that extract pricing data at infrastructure-consuming rates, and click-fraud bots that consume advertising budgets. Geographic traffic anomalies cost small operators with a purely national market server capacity. Some 40.7% of daily bot traffic originates from Ireland and 13% from Singapore, both cloud data centre regions with no plausible purchase intent for a DACH-focused merchant (DreamHost and Imperva, 2025).

5.6 Structural asymmetry: why SMEs are more exposed

Large retailers maintain customer-level return score profiles, benefit from collective intelligence through industry fraud databases, and employ dedicated loss prevention teams. ASOS, Zalando, and Amazon operate comparable systems requiring transactional data at scale. An operator processing 500 orders per month cannot derive robust return rate distributions from that volume. The Resource-Based View framework (Tantithamthavorn, Jiarpakdee and Croft, 2023) describes this as a capability gap. A small operator who knows what data to collect, and collects it consistently, has a capability that large operators pay a lot of money for in software, even if the data volume is modest.

5.7 Cost model

Table 2 sets out the modelled scenario parameters for a typical German micro-business webshop.

Parameter	Assumption
Monthly order volume	500 orders
Average order value	EUR 80
Gross margin	30% (EUR 24 per order)
Serial returner accounts	5 (1% of customer base)
Return rate, these accounts	70% of orders placed
Return rate, regular customers	10%
Processing cost per return	EUR 15
Resale rate on returned goods	50% (conservative)

Table 2. Baseline model parameters: micro-business SME webshop

At these parameters, five serial returner accounts ordering three times per month generate 10 to 11 returns per month. Direct processing costs: approximately EUR 158 per month. Goods value loss at 50%

resale rate: approximately EUR 400. Total monthly burden: approximately EUR 558, or EUR 6,696 annually. Annual revenue from these five accounts: approximately EUR 14,400. Net margin erosion: approximately 46%. Conventional cybersecurity has no answer to this. It is an economic problem with a legal dimension, caused by five customers acting entirely within their rights.

5.8 Legal countermeasures under EU law

The statutory 14-day withdrawal right is a hard constraint that cannot be shortened by terms and conditions. Within that constraint, operators have several options. Return shipping costs can be charged to the consumer if clearly stated in the withdrawal notice per Section 357(6) BGB and Article 14(1) of Directive 2011/83. Research consistently shows that return shipping charges reduce bracketing and wardrobing without eliminating legitimate returns (Merlano et al., 2024).

The ECJ judgment in Case C-97/22 (May 2023) established that demonstrably abusive exercises of the withdrawal right may be denied legal effect, provided the merchant documents the frequency and pattern of the consumer's return behaviour, the timing of withdrawals relative to the statutory deadline, and evidence that the conduct is inconsistent with the genuine need to inspect the goods (Laukemann, 2025). Customer-level return rate tracking falls within GDPR scope under Article 6(1)(f), the legitimate interest basis. The processing must be proportionate, limited to transaction history and return timing, and disclosed in the privacy notice.

5.9 Prevention strategies and ROI

The prerequisite for all prevention measures is customer-level return tracking. Every major e-commerce platform stores the data required to calculate return rates per account. What is missing is operator awareness, the data is already there. A monthly review of return rate per account, return reason distribution, timing of withdrawals relative to the statutory deadline, and products generating above-average return rates costs nothing but time and moves the operator from Endsley's first level of situation awareness to the second.

Charging return shipping requires only a pre-contractual disclosure change. Photograph documentation requirements for damage claims, implemented as a mandatory step in the returns portal before authorising a refund, deter friendly fraud and hardly bother honest claimants. Beck (2024/2025) found that mandatory evidence submission was among the most effective deterrents for casual fraud. A graduated return policy, applied to accounts in higher-risk tiers based on documented return history, allows operators to impose additional verification requirements on a small subset of accounts without affecting the majority of customers, with Section 307 BGB proportionality as the legal limit.

Cloudflare's free service tier provides bot filtering, rate limiting, and geographic access controls sufficient to eliminate unsophisticated bot traffic. Geographic filtering must whitelist search engine crawler user agents to avoid SEO damage. Combined mandatory return shipping plus photograph documentation, with an implementation cost of approximately EUR 100 in time, reduces the modelled monthly loss by approximately 40%, saving EUR 223 per month or EUR 2,676 annually. The measures pay for themselves within the first month.

6 Discussion

The analysis has four implications beyond the immediate findings. First, current SME cybersecurity guidance has a blind spot. Phishing simulations, patch management schedules, and basic network security hygiene do not address serial returning, bracketing, friendly fraud, or seller sabotage. A small webshop operator who implements all standard cybersecurity recommendations to the letter remains fully exposed to these threats.

Second, chambers of commerce and similar intermediary bodies are well placed to fill the gap. A tiered return policy template with GDPR-compliant documentation, a self-assessment tool for identifying

customer segments with elevated return risk, and a plain-language explanation of ECJ and BGH developments on withdrawal right abuse would cover ground that no current advisory service touches.

Third, the absence of SME-scale primary data in the return fraud literature is mainly a sampling problem. Academic studies use retailer survey networks that favour large operators. The population of firms most affected, sole traders and micro-businesses processing fewer than 1,000 orders per month, is almost entirely absent from the published evidence base. Recruiting through chambers of commerce is the way to reach them in the empirical phase.

Fourth, a proportionate regulatory response would clarify at directive level the evidentiary standard for merchant documentation of suspected abuse, and create a simplified mechanism for small operators to apply for withdrawal right restriction for documented repeat abusers. Neither Directive 2023/2673 nor Directive 2024/825, both currently being transposed into national law, addresses this imbalance.

7 Conclusion

This paper has made four contributions. It has proposed and developed the concept of behavioural threats to SME webshops as a distinct and so far little examined category of e-commerce risk. It has applied Routine Activity Theory and Situation Awareness Theory to explain both why this category disproportionately affects small operators and why even motivated operators fail to detect and respond effectively. It has analysed the EU legal landscape to identify countermeasures legally available to European merchants, including through the emerging ECJ doctrine on withdrawal right abuse. It has developed a prevention framework calibrated to the resource and capability constraints of micro-businesses, and shown that cheap guardianship improvements reduce exposure considerably.

Behavioural threats differ from technical threats in kind. They need a different analytical framework, a different evidence base, and different countermeasures, and they hardly appear in the research and guidance European SME webshop operators rely on. When five customers acting legally can erode 46% of annual margin, the answer has to be economic and legal. The planned empirical phase will test the analytical framework against primary qualitative data from German and Austrian micro-business operators recruited through chamber of commerce networks. In the end, this research will be judged by whether the guidance it produces reaches the small business owner who today has no name for the problem their five most difficult customers are creating.

References

Beck, A. (2024/2025) *Returns fraud and abuse: causes, patterns, responses*. European Council for Retail Loss. Available at: https://ecrloss.com

bevh and Oxford Economics (2025) *Die Bedeutung des E-Commerce für die deutsche Wirtschaft 2025*. Bundesverband E-Commerce und Versandhandel e.V.

Chargebacks911 (2024) *2024 chargeback field report*. Merchant Risk Council.

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.

DreamHost and Imperva (2025) *Bot traffic analysis and bad bot report 2025*.

Endsley, M.R. (1995) 'Toward a theory of situation awareness in dynamic systems', *Human Factors*, 37(1), pp. 32-64.

European Court of Justice (2023) *Case C-97/22*, judgment of 17 May.

European Parliament and Council (2011) *Directive 2011/83/EU on consumer rights*. OJ L 304, pp. 64-88.

European Parliament and Council (2016) *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation)*. OJ L 119, pp. 1-88.

European Parliament and Council (2018) *Regulation (EU) 2018/302 on addressing unjustified geo-blocking*.

European Parliament and Council (2023) *Directive (EU) 2023/2673 amending Directive 2011/83/EU as regards financial services contracts concluded at a distance*.

European Parliament and Council (2024) *Directive (EU) 2024/825 on empowering consumers for the green transition*.

HDI Versicherung and Sirius Campus (2022) *HDI Cyber-Studie: Cyberangriffe und Schäden bei KMU*. Available at: https://www.hdi.de

Johnson, S.D. and Nikolovska, M. (2022) 'The effect of COVID-19 restrictions on routine activities and online crime', *Journal of Quantitative Criminology*.

Laukemann, M. (2025) *Widerrufsrecht im Fernabsatz: Missbrauch möglich* [Online]. Anwalt.de.

Mastercard (2024) *Ecommerce fraud trends and statistics* [Online]. Available at: https://www.mastercard.com

Merchant Risk Council and Cybersource (2024) *2024 global eCommerce payments and fraud report*.

Merlano, E.F., Frei, R., Zhang, D., Murzacheva, E. and Wood, S. (2024) 'Consumer perspectives on interventions to combat fraudulent product returns', *International Journal of Physical Distribution and Logistics Management*, 54(10), pp. 969-1001.

National Retail Federation and Appriss Retail (2023) *2023 consumer returns in the retail industry*.

National Retail Federation and Appriss Retail (2024) *2024 consumer returns in the retail industry*.

National Retail Federation and Happy Returns (2025) *2025 retail returns landscape*.

ParcelLab and Statista (2023) *Regelung von Retourenkosten in den Top-Online-Shops in Deutschland 2023*.

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.

Rajapaksa, D. et al. (2024) *SME cybersecurity situational awareness*. Cited in Rombaldom, Becker and Johnson (2024).

Redo (2026) *Ecommerce returns statistics: key data for 2026* [Online]. Available at: https://redo.com/blogs/ecommerce-returns-statistics (Accessed: 22 September 2026)

Rombaldom, C., Becker, I. and Johnson, S.D. (2024) *A systematic review of SME cybersecurity*. Preprint [Online]. Available at: https://arxiv.org/pdf/2309.17186

Sectigo (2021) *State of website security and threat report*.

Sendcloud (2024) *E-Commerce-Lieferkompass 2023/2024*.

Tantithamthavorn, C., Jiarpakdee, J. and Croft, R. (2023) 'Cybersecurity resilience in SMEs', *Journal of Computer Information Systems*, 63(5).

Thales (2026) *2026 Bad Bot Report: bad bots in the agentic age*. Imperva [Online]. Available at: https://www.imperva.com/resources/resource-library/reports/2026-bad-bot-report/ (Accessed: 22 September 2026)

ZigZag and Retail Economics (2024) *Annual returns benchmark report 2024* [Online]. Available at: https://www.zigzag.global (Accessed: 22 September 2026)