2024 - The State of Cyber

Title: 2025_State_of_cyber/pdf
Date: 28th April 2025 Version: 1.0

Novalytics Limited

Cybersecurity in Europe 2024: The SME Challenge in Finance, Gambling, and Insurance

Novalytics Gibraltar

Abstract—The year 2024 was characterised by a marked increase in cybersecurity threats across Europe, notably impacting Small and Medium Enterprises (SMEs) operating within the finance, gambling / gambling, and insurance sectors. This paper provides an overview of cybersecurity in Europe during 2024, focussing on SMEs operating within these sectors. Key case studies highlight vulnerabilities in SMEs resulting from insufficient governance, outdated infrastructure, and limited defensive capabilities. The introduction of rigorous regulatory frameworks, such as NIS2 and DORA, has established cybersecurity accountability at the executive and board levels, making cybersecurity not just a technical concern but an imperative for governance. Implementing a Zero Trust architecture, improving identity and access management, automating vulnerability management, providing frequent security training, and regularly testing incident response plans are critical actions that demonstrably improve cyber posture.

Keywords—*Cybersecurity, Policy, Data Protection, DMARC, DKIM, Spoofing, Phishing*

Contents

Figure 1. ENISA Top Cyber Threats

1. Introduction

In 2024, cyber threats across Europe increased significantly, with Small and Medium-sized Enterprises (SMEs) experiencing a disproportionate share of the impact. This trend was particularly notable in sectors that handle sensitive financial and personal data, such as finance, gambling and gaming, and insurance. The year brought increased regulatory pressure, the emergence of new adversarial tactics, and continued geopolitical exploitation of cyber vulnerabilities.

Recent data from the European Union Agency for Cybersecurity (ENISA) confirm this escalation. ENISA's Threat Landscape 2023 report, covering incidents through early 2024, found that the most frequent threat types were distributed denial-of-service (DDoS) attacks, ransomware, and data breaches, with threat actors increasingly targeting availability and integrity of systems across the EU. The report concludes that both the number and the severity of incidents have increased compared to previous years [16].

In parallel, SMEs are less prepared to deal with these evolving risks. The World Economic Forum Global Cybersecurity Outlook 2024 identifies that twice as many small businesses as large enterprises report lacking the operational resilience needed to counter modern cyber threats. Key deficiencies include underinvestment in monitoring, fragmented governance, and excessive reliance on outdated systems and staff practices [17].

The financial sector, already highly digitised, has been further strained by the growing reliance on cloud infrastructure, the integration of fintech platforms, and increasingly complex third-party risk chains. These trends have widened the attack surface, allowing threat actors to exploit insecure APIs, the reuse of credentials, and phishing to compromise accounts [15].

In the gambling and gaming sectors, especially those operating under pan-European licencing frameworks, attackers launched large-scale DDoS campaigns in 2024. In particular, pro-Russian groups such as NoName057(16) targeted commercial gaming services in politically motivated incidents, demonstrating the increasing crossover between hacktivism and cybercrime [18].

In the insurance domain, while the demand for cyber coverage has increased, many providers remain vulnerable themselves. Regulatory stress testing and growing actuarial data have made it clear that insurers, especially smaller underwriters,are both targets and vectors for data breaches. The European cyber insurance market, which saw a 50% growth in premium volume in some regions, reflects both

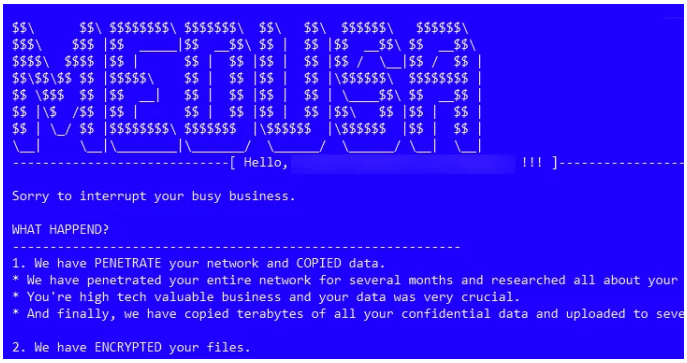

Figure 2. Medusa Ransomware Screenshot

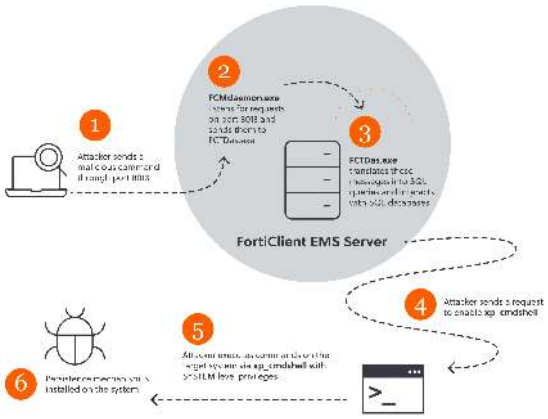

Figure 3. Supply chain Ransomware Attack - Fortigate Medusa attack

increased risk and greater awareness of sector exposure [19].

This document provides an overview of cybersecurity in Europe during 2024, focussing on SMEs operating within the finance, gambling / gambling, and insurance sectors. Examines the evolving threat environment, presents illustrative case studies, outlines practical mitigations, and concludes with recommended actions to build cyber resilience.

2. Threats

The European cyber threat landscape in 2024 was dominated by five interrelated vectors: ransomware-as-a-service (RaaS), DDoS attacks, third-party and supply chain compromises, credential phishing, and data integrity threats. These threats evolved in sophistication and scale, affecting both critical infrastructure and SMEs in sensitive data handling sectors.

2.1. Ransomware-as-a-Service (RaaS)

Ransomware operators increasingly adopted businesslike models, offering affiliate programmes that allowed nontechnical actors to deploy sophisticated payloads. The modularisation of ransomware kits allowed for faster campaign deployment and obfuscation of attribution. SMEs, particularly in the insurance and fintech ecosystems, were frequently targeted due to perceived underinvestment in backup, segmentation, and endpoint protection strategies [14].

2.2. Distributed Denial of Service (DDoS)

Europe saw an increase in ideologically motivated DDoS attacks, particularly in the context of regional political tensions. Groups such as NoName057(16) and Killnet leveraged botnets to target financial institutions, gambling platforms, and online insurance portals. These attacks, often used as cover for other intrusions, were noted for their duration and their use of layer 7 (application level) saturation techniques [9].

2.3. Supply Chain and Third-Party Risk

Threat actors increasingly targeted software vendors, cloud service providers, and managed security providers as a means to reach downstream SME clients. This trend mirrored the SolarWinds and Kaseya-style attacks observed in previous years. In 2024, SMEs in the financial sector that use third-party payment processors and identity verification services were disproportionately affected, often through indirect compromise of OAuth and SAML integrations [20].

2.4. Credential Harvesting and Phishing

Phishing attacks became more convincing with the help of generative AI, which enabled grammatical correctness, contextual tailoring, and spoofed domain authenticity. The finance and insurance sectors saw widespread credential reuse attacks, where leaked credentials from previous breaches were used to access internal services. These campaigns were often automated and relied on poorly configured multi-factor authentication systems [7].

2.5. Data Integrity and Manipulation Attacks

Whereas traditional data breaches sought exfiltration, 2024 saw a shift towards data tampering, particularly in sectors where trust and accuracy are paramount. In the insurance industry, there have been attempts to modify claims records and falsify actuarial input data. This subtle but damaging attack vector challenges standard forensic and audit protocols [11].

3. Examples and Case Studies

To understand the real-world impact of cyber threats in 2024, this section presents selected case studies from the finance, gambling / gambling and insurance sectors in Europe. These incidents illustrate both the diversity and severity of the attacks faced by small businesses.

3.1. Central European Gaming Platform: Prolonged DDoS Attack

A licenced online gambling platform based in Slovenia was the victim of a DDoS attack that lasted more than 72 hours, disrupting user logins and tournament operations. The campaign, claimed by NoName057(16), appeared politically motivated due to the firm's association with a pan-European digital policy initiative. The attack targeted application-level endpoints, using geo-distributed botnets. The reliance of the gaming company on a single upstream CDN vendor limited its mitigation options [21].

3.2. Financial Cooperative in Portugal: Ransomware Attack with Data Leak

A small financial cooperative serving agricultural communities in Portugal experienced a ransomware attack deployed via malicious macros embedded in a supplier invoice. The cooperative's backup systems were found to be incomplete, leading to extended downtime. Exfiltrated data, including member financial histories, was leaked online after the organisation refused to pay. The attack exploited unpatched vulnerabilities in their on-premises ERP system.

3.3. Nordic Insurance Broker: Integrity Manipulation Attempt

In an unusual case, a regional insurance broker in Sweden reported the detection of an attempted data integrity attack. Instead of data exfiltration, the intruders attempted to silently alter the claims histories within the broker's SQL database. The investigators traced the intrusion to a spear phishing campaign targeting claims managers. This marked one of the few confirmed cases of financially motivated data manipulation in the insurance sector, reinforcing the need for database-level auditing and the detection of behavioural anomalies.

These incidents demonstrate that even smaller companies, despite their lower public profiles, are frequently targeted for strategic gain. In each case, the attackers exploited basic oversights: poor access control, insufficient monitoring, third-party overtrust, or failure to patch critical software.

4. Mitigations

Mitigating cyber threats in SMEs, especially within the finance, gambling/gaming, and insurance sectors, requires a multi-layered approach that balances technical controls, organisational policies, and external support. Although no strategy guarantees immunity, several defensive measures have consistently demonstrated risk reduction when properly implemented and maintained.

4.1. Network Segmentation and Access Control

One of the most effective mitigation strategies is logical network segmentation. By isolating critical services, such as payment systems or policyholder databases, from general IT infrastructure, organisations limit lateral movement after initial compromise. When paired with role-based access controls and strict least-privilege policies, segmentation significantly reduces ransomware and risk of increased privileges [8].

4.2. Endpoint Detection and Response (EDR)

SMEs benefit greatly from deploying lightweight EDR platforms that provide behavioural analysis and forensic visibility. Modern EDR tools, especially those with machine learning baselines, are capable of detecting zero-day threats and anomalous insider activity in real time. This is especially important in sectors with limited security personnel and long patching cycles [6].

4.3. Multi-Factor Authentication (MFA) with Context-Aware Policies

The use of MFA is now standard; however, improperly implemented MFA can be circumvented through phishing, token replay, or push fatigue. Context-aware MFA, where authentication factors depend on user behaviour, IP reputation, or device risk, provides a stronger barrier to unauthorised access. SMEs in finance and insurance should, in particular, enforce MFA in all administrative and client-facing portals [12].

4.4. Regular Tabletop Exercises and Incident Response Planning

Preparation significantly affects the outcome of a breach. SMEs that conduct periodic tabletop exercises simulate attack scenarios and ensure familiarity with incident response roles and escalation paths. These exercises have been shown to reduce the mean time to detect (MTTD) and the mean time to respond (MTTR), limiting operational and reputational damage [4].

4.5. Secure Software Supply Chain Practices

Supply chain compromise continues to be a key risk. SMEs relying on SaaS and cloud-based platforms must implement software bill of materials (SBOM) policies, perform vendor due diligence, and enforce code-signing verification. In regulated sectors such as insurance, these practices are becoming mandatory under EU compliance frameworks such as DORA and NIS2 [1].

4.6. Data Backups and Restoration Testing

Resilience to ransomware and destructive attacks is heavily dependent on reliable and regularly tested backups. Best practice dictates that backups be immutable, stored off-network, and subject to periodic integrity verification. Automated backup restoration testing is essential to validate that business continuity objectives can be met during a crisis [2].

Collectively, these mitigations form the basis for a resilient posture. However, they must be tailored to each organisation's risk profile, regulatory environment, and resource constraints. In SMEs, prioritisation and external advisory support are often required to ensure cost-effective implementation.

5. Importance of Accountability and Responsibility

As cyber threats increase in volume and sophistication, the need for clear accountability and institutional responsibility has grown. This is especially critical in Small and Medium Enterprises (SMEs), where resource limitations and informal governance structures often result in fragmented security ownership. In high-risk sectors such as finance, gambling / gambling, and insurance, regulatory frameworks are evolving to enforce not only technical compliance but also accountability at the executive and board level.

5.1. Regulatory Mandates on Governance

The European Union's revised Network and Information Security Directive (NIS2), in force as of 2024, places direct responsibility for cybersecurity on company directors. Failure to implement appropriate technical and organisational measures can result in personal liability, particularly in regulated industries. The directive demands that senior management be involved in the decision-making on cybersecurity risk, an approach supported by empirical studies linking board-level involvement with lower breach costs and shorter recovery times [3].

5.2. Security is a Leadership Issue

Academic research consistently shows that cybersecurity outcomes improve when leadership understands and embraces its role in governance. Firms where executives take visible responsibility for cyber risk management, such as approving policies, chairing incident reviews, and setting risk appetites, are significantly more resilient to both internal and external threats [10]. In contrast, organisations that delegate all security responsibility to IT departments often suffer from blind spots in the risk of the business process.

5.3. Responsibility for Supply Chain Dependencies

In 2024, numerous SMEs experienced third-party breaches due to their reliance on vendors that lack transparent security controls. Regulatory bodies have responded by shifting some liability for vendor performance to the SME customer. This implies that due diligence, contractual enforcement, and post-contract monitoring are now legal and ethical responsibilities of the enterprise, not the supplier alone [5].

5.4. Cultural and Ethical Responsibility

Beyond regulatory and operational dimensions, cybersecurity is also an ethical responsibility. Enterprises, especially those in data-heavy sectors, are custodians of public trust. Mismanagement of personal or financial data erodes user confidence and damages the standing of the market. Embedding accountability into organisational culture, for example, through regular policy reviews, breach drills, and named data protection officers, is essential to long-term trustworthiness [13].

5.5. Transparency and Post-Breach Disclosure

The post-incident response must include timely and accurate disclosure. European jurisprudence increasingly favours public and regulator notification within 72 hours of breach discovery. Failure to do so can cause reputational damage and loss of insurability. Transparency itself, when executed responsibly, is seen to reduce the long-term legal and financial consequences.

In short, accountability must extend beyond compliance. True resilience is built when responsibility for cyber risk is embedded at every level, from procurement officers and system architects to CEOs and board members.

6. Top Five Actions That Improve Your Posture

For SMEs operating in high-risk sectors such as finance, gambling / gambling and insurance, prioritising security initiatives is essential. Based on empirical evidence and sectoral studies, the following five

actions represent the most impactful and feasible improvements to cybersecurity posture.

6.1. Implement Zero Trust Network Architecture (ZTNA)

Zero-trust principles, wherein no entity is trusted by default, regardless of location, offer significant risk reduction by segmenting access and validating every request. ZTNA mitigates lateral movement in the event of a breach and reduces the attack surface of legacy networks. Research indicates that organisations adopting ZTNA experience fewer successful data breaches and better incident containment metrics.

6.2. Enforce Strong Identity and Access Management (IAM)

Centralising identity through modern IAM solutions with granular policies ensures that users have only the necessary access for their roles. Enhancements such as time-limited permissions, passwordless authentication, and identity federation are particularly effective in reducing credential-based compromise. These controls are cost-effective and scalable for SMEs.

6.3. Automate Vulnerability Management and Patch Deployment

Delayed patching remains one of the most exploited weaknesses. SMEs can deploy automated vulnerability scanners and use scheduled patch management tools to quickly remediate known vulnerabilities. Sector-specific studies confirm that automated patching reduces exploit rates by more than 60% compared to manual or ad hoc approaches.

6.4. Conduct Frequent and Realistic Security Awareness Training

Humans remain a critical attack vector. Studies show that regular training, particularly those using phishing simulations and context-sensitive microlearning, can reduce click rates on malicious links by over 40%. SMEs that incorporate training into onboarding and quarterly refreshers report improved detection of social engineering attempts.

6.5. Establish and Test an Incident Response Plan

A written and rehearsed incident response (IR) plan ensures operational continuity when an attack occurs. SMEs with tested IR plans recover faster and incur lower costs than those improvising during crises. Effective IR planning includes role assignment, third-party contacts, escalation paths, and post-incident reviews.

7. Summary

The year 2024 was characterised by a marked increase in cybersecurity threats across Europe, notably impacting Small and Medium Enterprises (SMEs) within the finance, gambling/gaming and insurance sectors. Persistent threat actors exploited vulnerabilities such as weak access control, poorly secured third-party relationships, and inadequate security awareness. SMEs faced intensified ransomware, DDoS attacks, supply chain compromises, sophisticated credential phishing, and unprecedented data integrity attacks.

Key case studies highlighted vulnerabilities in SMEs resulting from insufficient governance, outdated infrastructure, and limited defensive capabilities. The introduction of rigorous regulatory frameworks, such as NIS2 and DORA, has established cybersecurity accountability at the executive and board levels, making cybersecurity not just a technical concern but an imperative for governance.

To strengthen resilience, SMEs are urged to adopt practical and evidence-based mitigations. Implementing a Zero Trust architecture, improving identity and access management, automating vulnerability management, providing frequent security training, and regularly testing incident response plans are critical actions that demonstrably improve cyber posture.

The responsibility for robust cybersecurity lies with the organisational leadership, who must actively promote security as an integral element of corporate governance and culture. Only through proactive measures, embedded accountability, and continuous monitoring can SMEs effectively manage cyber risk and protect their operations, reputation, and customers.

Contact Novalytics for More Information

Novalytics specialises in cybersecurity, information governance, and advanced analytics solutions designed specifically for SMEs operating within high-risk sectors. Our experts provide personalised guidance, strategic insight, and practical support to protect your organisation against evolving cyber threats.

For additional details on cybersecurity best practices, assistance with regulatory compliance, or a consultation on improving your organisation's cyber resilience, please contact us via:

- Website: https://www.novalytics.com
- Email: contact@novalytics.com

References

[1] R. J. Ellison, J. B. Goodenough, C. B. Weinstock, and C. Woody, "Evaluating and mitigating software supply chain security risks," *Software Engineering Institute, Tech. Rep. CMU/SEI-2010-TN-016*, 2010.

[2] R. Xia, X. Yin, J. A. Lopez, F. Machida, and K. S. Trivedi, "Performance and availability modeling of itsystems with data backup and restore," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 4, pp. 375–389, 2013.

[3] M. Schallbruch, *The european network and information security directive–a cornerstone of the digital single market*, 2018.

[4] G. N. Angafor, I. Yevseyeva, and Y. He, "Game-based learning: A review of tabletop exercises for cybersecurity incident response training," *Security and privacy*, vol. 3, no. 6, e126, 2020.

[5] T. Sobb, B. Turnbull, and N. Moustafa, "Supply chain 4.0: A survey of cyber security challenges, solutions and future directions," *Electronics*, vol. 9, no. 11, p. 1864, 2020.

[6] A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, "Endpoint detection & response: A malware identification solution," pp. 1–8, 2021.

[7] Y. Al-Hamar, H. Kolivand, M. Tajdini, T. Saba, and V. Ramachandran, "Enterprise credential spear-phishing attack detection," *Computers & Electrical Engineering*, vol. 94, p. 107 363, 2021.

[8] W. R. Simpson and K. E. Foltz, "Network segmentation and zero trust architectures," pp. 201–206, 2021.

[9] A. Singh and B. B. Gupta, "Distributed denial-of-service (ddos) attacks and defense mechanisms in various web-enabled computing platforms: Issues, challenges, and future research directions," *International Journal on Semantic Web and Information Systems (IJSWIS)*, vol. 18, no. 1, pp. 1–43, 2022.

[10] W. J. Triplett, "Addressing human factors in cybersecurity leadership," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 573–586, 2022.

[11] Z. Chang, J. Wu, H. Liang, Y. Wang, Y. Wang, and X. Xiong, "A review of power system false data attack detection technology based on big data," *Information*, vol. 15, no. 8, p. 439, 2024.

[12] S. R. Kandula, N. Kassetty, K. S. ALANG, and P. Pandey, "Context-aware multi-factor authentication in zero trust architecture: Enhancing security through adaptive authentication," *International Journal of Global Innovations and Solutions (IJGIS)*, 2024.

[13] S. Miller and T. Bossomaier, *Cybersecurity, ethics, and collective responsibility*, 2024.

[14] C. Patsakis, D. Arroyo, and F. Casino, "The malware as a service ecosystem," pp. 371–394, 2024.

[15] U. J. Umoga, E. O. Sodiya, O. O. Amoo, and A. Atadoga, *A critical review of emerging cybersecurity threats in financial technologies*, 2024.

[16] *ENISA Threat Landscape 2024 | ENISA*, [Online; accessed 28. Apr. 2025], Apr. 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[17] *Global Cybersecurity Outlook 2025*, [Online; accessed 28. Apr. 2025], Jan. 2025. [Online]. Available: https://www.weforum.org/publications/global-cybersecurity-outlook-2025.

[18] M. Nawrocki, C. Conrad, and C. A. NETSCOUT, *Campaign analysis noname057 hacker in a hoody–global security mag online*, 2025.

[19] S. Panda, A. Farao, E. Panaousis, and C. Xenakis, "Cyber-insurance: Past, present and future," pp. 529–532, 2025.

[20] Z. Tan, S. P. Parambath, C. Anagnostopoulos, J. Singer, and A. K. Marnerides, "Advanced persistent threats based on supply chain vulnerabilities: Challenges, solutions & future directions," *IEEE Internet of Things Journal*, 2025.

[21] "Tempo Hit by Massive DDoS Cyber Attacks Following Online Gambling Coverage - News En.tempo.co," Apr. 2025, [Online; accessed 28. Apr. 2025]. [Online]. Available: https://en.tempo.co/amp/1995461/tempo-hit-by-massive-ddos-cyber-attacks-following-online-gambling-coverage.


novalytics