Applied Studies in Agribusiness and Commerce – APSTRACT
University of Debrecen, Faculty of Economics and Business, Debrecen
SCIENTIFIC PAPERS
DOI: 10.19041/APSTRACT/2026/1/6

CYBER MATURITY AMONG EUROPEAN SMES: A TIME-SERIES AND CLUSTER-BASED ANALYSIS

Zsanett Porkoláb-Angyalos[1], Róbert Szilágyi[2]

[1,2]University of Debrecen, Institute of Methodology and Business Digitalization

[1]Corresponding author e-mail address: zsanett.angyalos@gmail.com

Abstract: *This study examines the macro-level evolution of cybersecurity maturity among European small and medium-sized enterprises (SMEs) between 2015 and 2025, with particular focus on trends in cyber threat exposure, defensive investment patterns, and the regulatory impact of the NIS2 Directive. Given the limited availability of long-term firm-level microdata, the research combines aggregated EU-level time-series data (Eurostat, ENISA, IBM) with a calibrated synthetic SME dataset (N = 100) to model maturity dynamics. Time-series forecasting was conducted using Prophet models to analyze the development of incident frequency (INCID_FREQ) and cybersecurity investment intensity (SPEND_RATIO), treating NIS2 as an exogenous regulatory shock. In parallel, K-Means clustering was applied across three maturity dimensions (investment ratio, NIS2 compliance level, and incident response time) to identify distinct cybersecurity profiles. The results indicate that cyber threat exposure has increased at a faster pace than defensive expenditures, particularly between 2015 and 2020. While the anticipated NIS2 effect in 2025 generates a measurable surge in security spending, it does not ensure long-term convergence between risk growth and investment intensity. The cluster analysis identifies three maturity groups (Ad-hoc, Managed, and Optimized) corresponding to consolidated CMMI and NIST-CSF levels. These findings suggest that regulatory pressure can accelerate short-term adaptation, but sustainable cybersecurity maturity among SMEs requires structural capability development, governance improvements, and strategic investment alignment*

Keywords: *Cybersecurity; SMEs; Cyber attacks; Digital security*
(JEL code: M15, O33, D22, O38)

INTRODUCTION

The exponential growth of the digital economy over the past decade has fundamentally transformed the operational logic and value-creation mechanisms of European enterprises. The technological advancements of the Fourth Industrial Revolution (Industry 4.0), including cloud computing, Big Data analytics, and the integration of artificial intelligence (AI), no longer merely provide a competitive advantage but have become a prerequisite for market participation.

At the same time, however, the spread of technological innovation and data-driven business models has dramatically increased organizations' exposure to cyber threats. (Eurofound and Cedefop, 2025) As a recent OECD analysis highlights, the importance of cybersecurity protection is steadily increasing as digital technologies become deeply embedded in critical sectors of the economy; in parallel, both the frequency of cyberattacks and the costs of disruptions are rising. As emphasized by the research of Seed et al. (2023), the strategic significance of cybersecurity continues to grow, and corporate value creation is now inseparable from information security maturity.

An examination of the structure of the European economy reveals that small and medium-sized enterprises (SMEs) constitute its backbone. According to Eurostat (2024), more than 99% of enterprises in the European Union belong to this sector, providing nearly two-thirds of total employment and generating a substantial share of added value.

Consequently, the cyber resilience of the SME sector is not merely a firm-level risk management issue but also a factor of macroeconomic stability. The sector faces a dual challenge: digital transformation is unavoidable in order to maintain market competitiveness, yet most enterprises operate with limited financial and human resources to develop and sustain advanced cybersecurity solutions. (Yigit Ozkan, B., & Spruit, M., 2022)

While multinational corporations and operators of critical infrastructure have progressively developed sophisticated, multi-layered defense mechanisms (defense-in-depth), the SME sector lags significantly behind in terms of cybersecurity maturity. Numerous studies indicate that SMEs typically lack adequately trained professionals, documented processes, and dedicated IT budgets, resulting in a security gap compared to large enterprises. (Heidt et al., 2019)

This "security gap" generates asymmetric risk: attackers increasingly target less protected SMEs, often using them as

entry points for supply chain attacks against larger corporations. (Elena Kaiser, 2023)

Despite the outstanding economic importance of SMEs, measuring the sector's cyber resilience faces structural challenges, particularly with regard to time-series data. While systematic data are available for large-scale operators of essential services (OES), statistical data collection within the SME sector remains fragmented and incomplete.

The study seeks to answer the following research questions:

1. How did trends in cybersecurity threat exposure and defensive expenditures evolve among European SMEs between 2015 and 2025?

2. What impact has the NIS2 Directive had on the development of cybersecurity among European SMEs?

3. Can clearly distinct maturity clusters be identified among SMEs, and how can these be characterized?

LITERATURE REVIEW

SMEs and Cybersecurity Challenges

European small and medium-sized enterprises (SMEs) continue to operate in a complex economic environment. In recent years, geopolitical tensions, particularly the Russian–Ukrainian war, high energy prices, inflation, and disruptions in supply chains have significantly affected their operations. Global economic prospects remain uncertain, while international trade tensions and changes in tariff regimes pose additional downside risks (European Commission, 2024).

Despite these adverse conditions, SMEs continue to play a decisive role in the EU economy. In 2024, approximately 26.1 million enterprises operated in the non-financial business sector, with projected growth of 1.2% by 2025 (European Commission, 2024). Microenterprises are particularly dynamic: their real value added is expected to increase by 2.2% by 2025, indicating that the sector retains a certain degree of adaptive capacity.

Table 1. Economic structure of enterprises by size class in the EU, 2024

Class size	Number of enterprises	Share (%)	Persons employed	Share (%)	Real Value Added (Billion €)	Share (%)
Micro	24,514,649	93.6%	41,540,252	30.1%	1,538	20.1%
Small	1,404,631	5.4%	26,889,824	19.5%	1,273	16.6%
Medium-sized	214,000	0.8%	21,358,947	15.5%	1,293	16.9%
SMEs (total)	**26,133,280**	**99.8%**	**89,789,023**	**65.1%**	**4,104**	**53.6%**
Large	44,358	0.2%	48,039,714	34.9%	3,559	46.4%
Total	**26,177,638**	**100%**	**137,828,737**	**100%**	**7,663**	**100%**

Source: JRC calculations based on Eurostat's Structural Business Statistics, Short-Term Business Statistics, and National Accounts Database

This resilience, however, is grounded not only in financial and organizational capacity but also in digital preparedness and cybersecurity readiness. More than half of SMEs lack a formal cybersecurity plan or dedicated specialist (ENISA SME Survey, 2022), while the proportion of cyberattacks continues to increase year by year.

At this point, the concept of cyber resilience becomes central: it encompasses not only prevention but also rapid recovery following attacks and the systematic incorporation of lessons learned.

The IBM Cost of a Data Breach Report 2024 highlights that post-incident recovery is a lengthy and complex process for most organizations. According to the report, only 12% of affected organizations reported full recovery. Among surveyed companies, 78% required more than 100 days to recover, while more than one-third needed over 150 days to achieve full restoration (IBM, Cost of a Data Breach Report, 2024). The term "recovery time" in the report does not refer solely to the technical restoration of IT systems but to the broader organizational regeneration process, including the settlement of fines and compensation, as well as the fulfillment of compliance obligations.

An organization's cyber resilience is closely linked to its cybersecurity maturity, which reflects the extent to which risks are managed consciously and systematically. Prominent maturity models, such as CMMI, the NIST Cybersecurity Framework (NIST CSF), ISO/IEC 27001, and the ENISA SME Assessment Tool, share the common premise that cybersecurity constitutes a developable organizational capability across technological infrastructure, governance processes, human factors, and incident response. Enhancing cybersecurity maturity is therefore a fundamental prerequisite for the sustainable digital transformation of SMEs.

AI-Driven Attacks and the Risk of Shadow AI

In recent years, a clear trend has emerged: artificial intelligence (AI) not only strengthens defensive mechanisms, through faster detection and response capabilities, but has also become embedded in attackers' toolkits. Certain analyses indicate that the application of cybersecurity automation and AI can significantly reduce the scale of damages. According to IBM's 2025 data, organizations extensively using AI and automation experienced, on average, USD 1.9 million

lower incident costs, and the lifecycle of a cyberattack (from detection to containment) was shortened by 80 days.

At the same time, AI has become an effective weapon in the hands of adversaries. IBM's 2025 report notes that in 16% of the analyzed data breaches, attackers employed some form of AI tool, most commonly for phishing purposes.

For SMEs, a particularly critical risk is so-called Shadow AI, that is, the use of unauthorized AI tools operating outside formal organizational oversight. According to IBM data, incidents linked to Shadow AI accounted for 20% of all data breaches. This risk is further amplified by the fact that 63% of organizations either lack a formal AI governance policy or are only in the process of developing one.

These findings underscore that, in the future, SMEs must not only strengthen traditional IT security practices but also address the security implications of AI adoption and governance in a systematic manner (IBM Newsroom, 2025).

European Policy and Regulatory Environment

The European Union has recognized that enhancing cybersecurity maturity is essential for the competitiveness and resilience of the digital economy. The NIS2 Directive was adopted by the European Union in December 2022 and entered into force on 16 January 2023, while Member States were required to transpose the directive into national law by 17 October 2024. The directive mandates that each Member State adopt a national cybersecurity strategy, including provisions on supply chain security, vulnerability management, as well as education and awareness-raising programs. Compared to the previous NIS1 framework, the new directive introduces a broader scope, clearer regulatory requirements, and stricter supervisory and enforcement mechanisms.

Sectoral extension: In addition to previously covered critical infrastructures (energy, transport, finance, healthcare, drinking water, and digital infrastructure), the directive now also encompasses public electronic communications, digital services (e.g., online marketplaces and social platforms), waste management, critical product manufacturing, postal and courier services, central and regional public administration, and even the space sector.

Extension by size: As a general rule, NIS2 obliges all medium-sized and large entities operating in critical sectors to implement appropriate cyber risk management measures and to report any significant incidents to the competent authority.

In parallel, the EU has launched programs such as the Digital Europe Programme (2021–2027) and the Digital Decade 2030 initiative, which support the widespread adoption of digital technologies, including cybersecurity and artificial intelligence. Within these frameworks, SMEs receive particular emphasis through targeted funding instruments and expert support structures, such as the European Digital Innovation Hubs, to facilitate cybersecurity development.

The overarching objective is to ensure that SMEs do not merely react to evolving threats but proactively integrate into the broader digital and security ecosystem. Consequently, cybersecurity maturity is no longer solely a defensive factor but is increasingly becoming a prerequisite for competitiveness in the digital economy.

NIS2 as an Exogenous Shock

The NIS2 Directive clearly constitutes an external shock to the SME sector, exerting a coercive effect on security investments in certain respects. Its predecessor was the NIS1 Directive adopted by the European Union in 2016, which primarily focused on critical infrastructure and operators of essential services, leaving the majority of SMEs outside its direct scope. However, the acceleration of digitalization and the growing vulnerability of supply chains exposed the limitations of this framework, ultimately leading to the adoption of NIS2.

With its expanded scope and more stringent requirements, NIS2 represents a tangible exogenous shock for the SME sector. The new regulation introduces strict compliance and incident-reporting obligations, including notification to the competent authority within 72 hours of a significant incident, the requirement to conduct independent cybersecurity audits every two years, and the provision of continuous employee training (EU NIS, 2022). These obligations, along with the prospect of substantial fines for non-compliance, constitute primary incentives for SMEs to increase cybersecurity expenditures.

Importantly, NIS2 is not merely a legal obligation; in practice, it is increasingly becoming a prerequisite for entering or remaining within supply chains. Large enterprises falling under the scope of NIS2 (so-called essential and important entities) are responsible for the security of their entire supply chains and therefore expect compliance from their SME partners, often in the form of security audits. This market-driven pressure represents an indirect yet indispensable driver of cybersecurity maturity growth.

It is already observable that consulting firms are approached by companies that, while not directly subject to NIS2, serve as suppliers to large enterprises that are. (RealCob, 2025). These major partners seek to assess their subcontractors' cybersecurity posture or require formal declarations of compliance with NIS2 requirements. For suppliers, the outcomes of such audits are critical, as they may directly affect future business opportunities, including tenders and contractual engagements. Thus, even where legal compliance with NIS2 is not yet mandatory, competitive pressure and the need to maintain cooperation with larger partners compel SMEs to implement security improvements and standardize their systems.

Overall, the cybersecurity maturity of SMEs is shaped by a complex set of factors: internal resources and awareness levels, rapidly evolving threat landscapes (e.g., AI-driven attacks), as well as the regulatory and market environment all exert significant influence.

Based on the review of theoretical models and the relevant literature, it is evident that the cybersecurity maturity of SMEs is influenced by a range of interrelated factors, from technological advancement and regulatory pressure to organizational awareness. At the same time, publicly available, long-term micro-level data suitable for quantitative analysis are typically lacking, particularly with a specific focus on the SME segment.

To address this limitation, the present study employs syn-

thetic indicators calibrated to reflect real-world trends in order to map the temporal evolution of cybersecurity maturity and its principal determinants. The methodology presented in the following section aims to explore SMEs' security investment patterns, resilience characteristics, and the potential impact of the NIS2 regulation through statistical modeling.

MATERIALS AND METHODS

This study applies a predominantly quantitative research design. The qualitative elements are limited to the conceptual interpretation of cybersecurity maturity frameworks and policy implications related to NIS2.

Data Sources and Time Interval

The objective of this study is to explore macro-level changes in the cybersecurity environment of European small and medium-sized enterprises (SMEs), with particular emphasis on the evolution of security investments, trends in incident frequency, and the potential impact of the regulatory environment, primarily the NIS2 Directive, over the 2015-2025 period.

The quantitative analysis is constrained by the lack of publicly available, long-term, firm-level microdata on cybersecurity maturity within the EU SME sector. To address this limitation, the study employs proxy indicators derived from consolidated macro-level data sources, along with a calibrated synthetic firm-level dataset. The proxy-based approach was adopted because harmonized, long-term, firm-level cybersecurity maturity data for European SMEs are not publicly available. The purpose of the synthetic dataset is not to precisely replicate the actual SME population, but rather to generate plausible distributions suitable for the statistical identification and comparison of cybersecurity maturity clusters.

The synthetic database represents N = 100 European SMEs, each assigned an EU Member State country code and an economic sector classification. The sample includes ten sectors commonly represented among SMEs (e.g., manufacturing, ICT services, financial services, healthcare, trade, logistics). During data generation, firms were constructed from three sampling segments reflecting different cybersecurity maturity levels (low, medium, and high maturity), in approximately 40-40-20% proportions. These proportions served solely for calibration purposes and were not directly imposed on the clustering algorithm; maturity clusters were determined in a fully data-driven manner based on the input variables using the K-Means algorithm.

The dataset operationalizes three key dimensions of cybersecurity maturity:

- SPEND_RATIO - the proportion of information security expenditures within the total IT budget (%),
- NIS2_COMP - the estimated proportion of implemented mandatory measures associated with the NIS2 Directive (%),
- INCID_TIME - the time required to detect and contain cybersecurity incidents (days).

Theoretical Justification of Maturity Variables

Cybersecurity maturity is a multidimensional organizational capability that encompasses technological preparedness, governance structures, incident response capacity, and continuous improvement mechanisms. In order to operationalize these dimensions within the SME context, the present study applies three proxy variables derived from established cybersecurity maturity frameworks, primarily the NIST Cybersecurity Framework (NIST CSF) and the Capability Maturity Model Integration (CMMI).

The variable SPEND_RATIO, representing the proportion of cybersecurity expenditures within the total IT budget, serves as an indicator of technological and organizational capability development. Previous studies suggest that cybersecurity investment intensity reflects the extent to which organizations prioritize security capacity-building, infrastructure modernization, and preventive controls (Heidt et al., 2019; ENISA, 2024). Within the logic of the NIST CSF, this variable is primarily associated with the Protect function, while in the CMMI framework it reflects the transition from ad hoc security practices toward more managed and optimized processes.

The variable NIS2_COMP captures the estimated level of implementation of mandatory cybersecurity measures associated with the NIS2 Directive. This variable reflects governance maturity, regulatory preparedness, and the formalization of cybersecurity processes. In conceptual terms, it corresponds to the Identify and Govern dimensions of cybersecurity management within the NIST CSF logic, including risk assessment, policy implementation, and compliance monitoring. From a CMMI perspective, higher levels of NIS2 compliance indicate increasing process formalization and institutionalization.

The variable INCID_TIME, measuring the time required to detect and contain cybersecurity incidents, represents organizational resilience and operational response capability. Incident response speed is widely recognized as a critical dimension of cybersecurity effectiveness, particularly in relation to business continuity and recovery performance (IBM Security, 2024). Within the NIST CSF framework, this variable is linked to the Detect, Respond, and Recover functions, while in the CMMI maturity logic it reflects the degree to which organizations possess repeatable and optimized incident management processes.

Taken together, these three variables provide a multidimensional approximation of SME cybersecurity maturity by integrating technological capability (SPEND_RATIO), governance and compliance readiness (NIS2_COMP), and operational resilience (INCID_TIME). Although the study relies on proxy indicators and synthetic firm-level data, the selected variables are conceptually grounded in established cybersecurity maturity frameworks and calibrated using empirically observed distributions reported by ENISA, IBM, and related European cybersecurity studies.

Variable Calibration and Data Construction

The variables were sampled from differently parameterized distributions to ensure realistic heterogeneity aligned

with varying SME cybersecurity maturity levels. However, cluster determination relied exclusively on the results of the data-driven K-Means algorithm. Parameter ranges were calibrated based on ENISA NIS Investments reports (investment ratios and dispersion), ENISA NIS implementation experience and preparedness surveys (NIS2 compliance), and IBM Cost of a Data Breach reports (scaled components of incident detection and response times).

The SPEND_RATIO variable measures the share of information security expenditure within the total IT budget (%), with its distribution calibrated to EU median values reported by ENISA (approximately 5-13%) and the broader variance observed among SMEs.

The resulting dataset served as the basis for cybersecurity maturity cluster analysis, while the time-series analyses rely exclusively on actual macro-level data from Eurostat, ENISA, and IBM

The synthetic dataset does not aim to reproduce the actual SME population, but to approximate plausible maturity distributions based on published aggregate indicators.

Table 2. Operationalization of Variables Using a Proxy Approach

Category	Variable (Proxy)	Operationalization (Measurement)	Objective within the Maturity Model
Cybersecurity Maturity (CYB_MAT)	CYB_CLASS (Cluster Variable)	1, 2, 3 (cybersecurity maturity profiles identified through data-driven K-Means cluster analysis)	Process, Capability dimension
Investment Capacity	SPEND_RATIO	Share of cybersecurity expenditures relative to total IT spending (estimated ratios based on ENISA and IBM data)	Technological, Capability dimension
Risk Exposure	INCID_FREQ (Time Series)	Annual Incident Frequency Index (primarily ransomware and phishing incidents)	Resilience, Detection dimension
NIS2 Compliance	NIS2_COMP	Estimated proportion of implementation of the 10 mandatory NIS2 measures (%)	Organizational, Process dimension

Source: Author's own compilation

Statistical Modeling

The objective of the time-series analysis is to dynamically examine trends in cybersecurity investments and threat exposure among SMEs over the 2015–2025 period. The analysis employs the Prophet model to identify temporal patterns, long-term trends, and potential structural breakpoints. The introduction of the NIS2 Directive is treated as an external (exogenous) event that may influence the evolution of variables representing cybersecurity maturity.

The model is based on two primary indicators:

- INCID_FREQ: the annual percentage of SMEs reporting at least one significant ICT security incident (including ransomware, phishing, and DDoS events), based on aggregated Eurostat and ENISA data;
- SPEND_RATIO: the proportion of cybersecurity investments within total IT expenditure (Eurostat).

The dataset covers the period from 2015 to 2024, with the model generating forecasts for 2025-2026.

To assess short-term forecast reliability, a one-step-ahead rolling backtest was conducted for both time-series models. Forecast accuracy was evaluated using Mean Absolute Error (MAE), expressed in percentage points. The backtest results indicate an average absolute deviation of 1.32 percentage points for INCID_FREQ and 1.18 percentage points for SPEND_RATIO. Given the annual frequency and limited sample size, this error magnitude suggests a reasonably stable short-term predictive performance and supports the interpretability of the projected trends.

In order to ensure a holistic approach to cybersecurity maturity, drawing conceptually on the CMMI and NIST Cybersecurity Framework (NIST CSF), K-Means clustering was applied. K-Means was selected because it provides an interpretable unsupervised classification method for identifying homogeneous groups based on numerical cybersecurity maturity variables. The number of clusters was set to k = 3 based on the three-tier maturity logic adopted in this study, informed by established cybersecurity maturity frameworks such as CMMI and NIST CSF.

The clustering procedure was conducted along three principal dimensions that collectively capture the critical components of maturity:

- SPEND_RATIO (the proportion of security expenditures within the total IT budget),
- NIS2_COMP (level of preparedness for NIS2 compliance), and
- INCID_TIME (time required for incident detection and containment).

This clustering approach enables the identification of distinct SME maturity profiles based on multidimensional cybersecurity characteristics.

RESULTS AND DISCUSSION

Time-Series Analysis of European SME Cybersecurity Trends (2015–2025)

The time-series analysis database consists of annual-frequency, aggregated indicators at the European SME level covering the 2015-2025 period.

The analysis was based on two key indicators:

- INCID_FREQ: The annual incidence rate of reported IT security incidents affecting small and medium-sized enterprises (SMEs) operating within the EU.
- SPEND_RATIO: The proportion of IT security expenditures within the total corporate IT budget.

Trend Analysis and Forecasting

The evolution of cyber threat exposure (INCID_FREQ) was examined using a linear Prophet model, while the growth of security expenditures (SPEND_RATIO) was modeled with a logistic curve, incorporating the expected impact of the NIS2 Directive entering into force in 2025.

Given the limited number of annual observations, the Prophet model for INCID_FREQ was primarily applied as a trend-fitting and short-term forecasting tool.

Key Findings

- INCID_FREQ nearly doubled between 2015 and 2020 (from approximately 7.5% to around 15%), reaching 21.5% by 2023–2024, where it temporarily stabilized. The model estimates an incidence rate of approximately 23.7% for 2025 and 25.3% for 2026.
- SPEND_RATIO remained at roughly 5% in 2019 but increased to a median of 9% by 2023. Due to the projected NIS2 effect in 2025, the model estimates a one-time upward shift to approximately 12%, followed by a further increase to 13.1% in 2026.

The dynamic interaction of the two indicators suggests that the growth rate of cyber threat exposure exceeds the pace of defensive investment. However, the NIS2-related regulatory effect may temporarily accelerate adaptation within the SME sector.

Table 3. Summary Table of Time-Series Results

Year	INCID_FREQ (% of firms affected)	SPEND_RATIO (% of IT budget)	Remarks
2015	~7.5% (model baseline)	~3-5% (low level)	Cyber threat exposure still moderate; security spending minimal
2020	~15% (≈2× 2015)	~5.5%	Sharp increase in attacks; defensive investments lag behind
2023	21.5% (actual, Eurostat / ENISA)	9.0% (actual)	High incident rate; intensified focus on cybersecurity
2024	21.54% (actual, Eurostat 2024)	~9.5% (model estimate)	Incident rate stabilizing; gradual increase in spending
2025 (expected)	23.7% (Prophet forecast)	~12.1% (NIS2-driven one-time surge)	NIS2 compliance requirements → investment wave
2026 (expected)	25.3% (Prophet forecast)	~13.1% (logistic growth)	Persistently high threat level; security investment stabilizes at a higher plateau

Source: ENISA, Eurostat, IBM, OECD, and Prophet model estimations.

Context and Literature Background

The global economic cost of cybercrime had doubled by 2020 compared to its 2015 level, indicating that both the frequency and severity of attacks were still relatively moderate in 2015 (ENISA, 2024). During this period, organizations allocated on average only 3–5% of their total IT budgets to secu-

Table 4. Main Parameters of the Prophet Models (Time-Series Analysis)

Parameter	INCID_FREQ Model	SPEND_RATIO Model	Explanation
Model	Prophet	Prophet	Additive time-series model with trend + (optional) components
growth	linear (default)	logistic	Linear trend for incidents; saturating growth for expenditures
Capacity	–	cap = 15.0, floor = 0.0	Logistic growth with upper bound constraint
yearly_seasonality	False	False	Yearly seasonal component disabled (annual data points)
daily_seasonality	False	False	Daily seasonal component disabled
seasonality_mode	additive (default)	additive (default)	Additive treatment of seasonal effects (if applicable)
n_changepoints	25 (default)	25 (default)	Number of automatically detected trend changepoints
changepoint_range	0.8 (default)	0.95	Proportion of the time series in which changepoints are allowed
changepoint_prior_scale	0.05 (default)	0.6	Trend flexibility (higher value → more flexible trend)
Exogenous regressor	–	nis2	NIS2 proxy regressor (2024 = 0.3; 2025–2026 = 1.0)
nis2 prior	–	prior_scale = 5.0, additive	Strength (regularization) of the regressor's effect
interval_width	0.80 (default)	0.80 (default)	Width of the forecast confidence interval

Source: Author's own compilation.

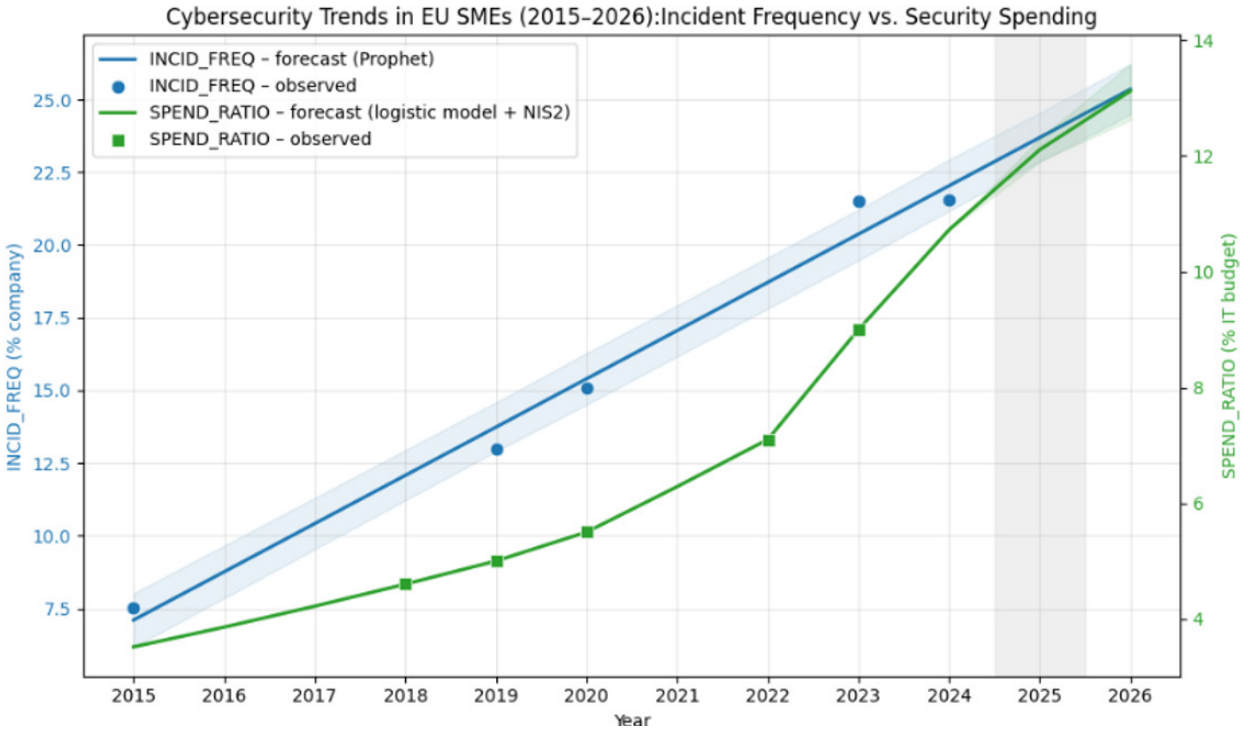
rity, meaning that defensive investments also started from a low baseline (NGA, 2019).

In Europe, by 2019 approximately 13% of enterprises had already experienced some form of ICT security incident, representing a significant increase compared to previous years (OECD, 2021). In contrast, the proportion of IT security spending rose only marginally from around 5%; in 2019 the median remained approximately 5%, and by 2020 it still hovered around 5–6% (Grillo & Dhifi, 2024). This divergence indicates that the growth in threat exposure was not matched proportionally by defensive investment.

According to the most recent data, in 2023 21.5% of EU enterprises experienced an ICT security incident, meaning that more than one in five firms were affected, representing a dramatic increase compared to the mid-2010s (Eurostat, 2023). In parallel, the share of spending dedicated to information security increased: in 2023, enterprises allocated a median of 9.0% of their IT budgets to cybersecurity (compared to approximately 7.1% in the previous year) (ENISA, 2024). Although security expenditure grew dynamically by 2023, it still lagged behind the pace of increasing threat exposure. This discrepancy can be explained by the severe wave of cyberattacks observed in the early 2020s, including ransomware campaigns and distributed denial-of-service (DDoS) attacks.

Looking ahead, cyberattacks are expected to continue rising: 90% of organizations anticipate further increases in attacks over the coming year (ENISA, 2024). With the entry into force of the NIS2 Directive in 2024, SMEs are also subject to mandatory minimum security requirements, which is likely to result in a one-time, and partly sustained, surge in defensive spending. According to ENISA's 2024 survey, most organizations expect to require additional budget allocations to achieve NIS2 compliance. As a result, by 2025 the share of IT security expenditures is projected to exceed 10% of total IT budgets. This may mark the first year in which growth in security investment, driven by regulatory pressure, keeps pace with the rising threat landscape.

Figure 1. Evolution and Forecast of INCID_FREQ and SPEND_RATIO (2015–2026)



Source: Author's own compilation.

The above figure illustrates the temporal evolution of cybersecurity threat exposure (INCID_FREQ) and the proportion of IT security expenditures (SPEND_RATIO) among European SMEs over the 2015-2026 period.

Based on the figure, the following patterns can be clearly observed:

- INCID_FREQ (threat exposure) shows a continuous upward trajectory, reaching approximately 25% by 2025-2026.
- SPEND_RATIO initially increases at a slower pace; however, as a result of the projected NIS2 effect in 2025, a significant surge in security investment occurs, approaching the 13% level.

The convergence of the two trends suggests that regulatory pressure may temporarily narrow the gap between rising threat exposure and defensive capacity.

Cluster Analysis of Cybersecurity Maturity Levels

K-Means clustering was performed along three key indicators that comprehensively capture cybersecurity maturity:

- SPEND_RATIO (the proportion of security expenditures within the total IT budget),
- NIS2_COMP (level of preparedness for NIS2 compliance), and
- INCID_TIME (time required for incident detection and containment).

Although the EU Cybersecurity Index (EU-CSI) and related surveys published by ENISA and Eurostat provide aggregated data on the cybersecurity status of the SME sector, such as incident prevalence rates and national medians, these datasets are typically aggregated at the Member State level and do not include publicly available firm-level microdata.

In the absence of such microdata, the present cluster analysis relies on a synthetic dataset calibrated to reflect real-world statistical distributions described in Eurostat, ENISA, and IBM reports. This approach enables SME-level cybersecurity maturity modeling while remaining aligned with empirically observed trends.

As a result, three maturity profiles emerged, consistent with the value ranges reported in published sources. The maturity levels assigned to the clusters are based on a combined interpretation of the CMMI (Capability Maturity Model Integration) and the NIST Cybersecurity Framework (CSF).

CMMI defines five maturity levels ("Initial," "Managed," "Defined," "Quantitatively Managed," and "Optimizing"), while NIST CSF distinguishes four implementation tiers ("Partial," "Risk-Informed," "Repeatable," and "Adaptive"). Both frameworks follow a comparable maturity logic. In the present analysis, these were consolidated into three levels aligned with SME practice:

- Level 1: Initial / Ad hoc,
- Level 2: Repeatable / Defined,
- Level 3: Managed / Optimized.

This three-tier scale is consistent with both CMMI and NIST maturity frameworks and provides a professionally grounded basis for describing cybersecurity maturity clusters. The distributions of the indicators were calibrated to ranges reported in recent ENISA, IBM, and JNGR research, ensuring that while the dataset is statistically synthetic, it reflects realistic and empirically grounded trends.

Table 5. Statistical Characteristics and Literature Alignment of Cybersecurity Maturity Groups Identified by K-Means Clustering

Indicator	Distribution / Logic (by Cluster)	Source / Rationale
SPEND_RATIO	Cluster I: <5% Cluster II: 5-10% Cluster III: >10%	ENISA NIS Investments 2021–2023, (median 6.7-9%, with wide dispersion among SMEs)
NIS2_COMP	Cluster I: <60% Cluster II: 60-75% Cluster III: >75%	ENISA NIS Implementation (2020) + JNGR 2025 preparedness study (48.5% vs. 72.3%)
INCID_TIME	Cluster I: >30 days Cluster II: 15-30 days Cluster III: <15 days	IBM 2024 (258-day global average breach lifecycle, scaled proportionally to detection & response phase)

Source: IBM, ENISA (2020)

The data-driven K-Means clustering applied to the synthetic dataset, calibrated to reflect real-world trends, identified three clearly distinguishable cybersecurity maturity profiles, which are presented in the following table.

Figure 2. Results of K-Means Clustering Among European SMEs - Median Values by Cluster

Median values by K-Means cluster

cluster_kmeans	n	spend_ratio_med	nis2_comp_med	incid_time_med
1	41	7.65	71.20	22.0
2	41	4.60	53.80	38.0
3	18	12.34	90.45	11.5

Source: Author's own compilation.

Table 6. Cybersecurity Maturity Profiles of Empirically Identified Clusters Based on Applied Maturity Models

Cluster	Maturity Level (CMMI/ NIST)	SPEND_ RATIO (IT Security / IT Budget)	NIS2_COMP	INCID_ TIME (Response Time)	Brief Characterization
I. Ad-hoc Protected	~1 (Initial)	Low	Low–Medium	Long	Low investment, limited compliance, slow response; high exposure and disproportionate compliance burden
II. Managed Processes	~2–3 (Repeatable / Defined)	Medium	Medium	Medium	Documented controls, improving maturity; frequent use of MSSP, EDR, and SIEM solutions
III. Optimized Resilience	~4–5 (Managed / Optimized)	High	High	Short	Mature processes, automation/ AI integration, practiced incident response playbooks; rapid detection and recovery

Source: Author's own compilation.

The cluster structure presented above is consistent with observed EU-level trends: median and average security expenditures have increased in recent years (ENISA); compliance levels vary significantly across sectors and firm sizes (transition from NIS to NIS2); and incident response times are substantially shorter among more mature, automated organizations (IBM). Given the absence of harmonized, publicly available European microdata on cybersecurity maturity, particularly within the SME sector, the model relies on a synthetic dataset calibrated to reflect empirically observed trends.

CONCLUSION

The aim of this study was to examine the macro-level cybersecurity maturity of European SMEs using synthetic data aligned with empirical trends. The research was built upon two principal methodological pillars: time-series forecasting and cluster-based maturity segmentation.

During the examined period (2015–2025), the growth of cyber threat exposure significantly outpaced the increase in defensive expenditures, particularly between 2015 and 2020. Although the NIS2 Directive, entering into force in 2024, triggered a one-time investment surge (as confirmed by the modeling results), it does not guarantee the sustained elevation of security spending levels. Nevertheless, regulatory pressure functions as a tangible incentive mechanism, demonstrably increasing IT security expenditures in quantitative terms.

The cluster analysis identified three clearly distinguishable cybersecurity maturity groups among SMEs (Ad-hoc, Managed, Optimized). These maturity tiers not only describe the heterogeneous defensive capabilities of organizations but also provide a structured basis for targeted policy interventions and support mechanisms.

In conclusion, the study demonstrates that while regulatory pressure can act as a catalyst for short-term improvements in cybersecurity spending, achieving sustained maturity requires a multifaceted approach that combines regulatory oversight with strategic investment incentives and capacity-building initiatives. The proposed maturity clusters offer a valuable tool for advancing evidence-based cybersecurity policy in the SME sector, contributing to both theoretical understanding and practical implementation.

REFERENCES

Amy Mahn (2018). Identify, Protect, Detect, Respond and Recover: The NIST Cybersecurity Framework, https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework, download: 2025.12.05

ENISA. (2024). NIS Investments 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf, download: 2025.12.05

ENISA: SMEs Cybersecurity - https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/smes-cybersecurity, download: 2025.12.05

ENISA. (2024). Report on the State of Cybersecurity in the Union. Publications Office of the European Union, Luxembourg. ISBN: 978-92-9204-681-1. https://doi.org/10.2824/0401593

ENISA. (2024). Threat Landscape 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 download: 2025.12.05

ENISA. (2021). Threat Landscape 2021. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202021.pdf, download: 2025.12.05

Elena Kaiser (2023). The new NIS II Directive and its impact on small and medium enterprises (SMEs): initial considerations,

European Commission: Directorate-General for Internal Market, Industry, Entrepreneurship,and SMEs. (2025). Annual report on European SMEs 2024/2025 – SME performance review 2024/2025. Publications Office of the European Union. 10.2760/7714438

European Commission. (2023). NIS2 Directive: Securing Network and Information Systems. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, download: 2025.12.05

Eurofound and Cedefop (2025). SME digitalisation in the EU: Trends, policies and impacts, Publications Office of the European Union, Luxembourg. DOI: 10.2806/8684886 ISBN: 978-92-897-2506

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. Information Systems Frontiers, 21(6), 1285–1305. 10.1007/s10796-019-09959-1

IBM Newsroom. (2025). IBM report: 13% of organizations reported breaches of AI models or applications, 97% of which reported lacking proper AI access controls. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications-97-of-which-reported-lacking-proper-ai-access-controls, download: 2025.12.05

RealCob (2025). Why NIS2 Matters for SMEs, Even If You're Not Directly Covered. https://realcob.com/blogs/nis2-for-smes-why-it-still-applies/, download: 2025.12.05

IBM Security. (2024). Cost of a Data Breach Report 2024. https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf, download: 2025.12.05

Grillo, L., & Dhifi, S. (2024). Cybersecurity budgets: Spend more or spend better? https://www.alvarezandmarsal.com/insights/cybersecurity-budgets-spend-more-or-spend-better, download: 2025.12.05

National Governors Association (2019). States Confront the Cyber Challenge Memo on State Cybersecurity Budgets. https://www.nga.org/wp-content/uploads/2019/09/State-Cyber-Budgets.pdf, download: 2025.12.05

OECD (2021). The digital transformation of SMEs. OECD Publishing. https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/02/the-digital-transformation-of-smes_ec3163f5/bdb9256a-en.pdf, download: 2025.12.05

OECD (2025). Economic Security in a Changing World, New Approaches to Economic Challenges, OECD Publishing, Paris, https://

doi.org/10.1787/4eac89c7-en.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, 23(15)10.3390/s23156666

Thapa, G., & Thapaliya, S. (2025). Cybersecurity Challenges in Small and Medium Enterprises (SMES) in Nepal. International Journal of Multidisciplinary and Innovative Research, 0210.58806/ijmir.2025.v2i6n05

Yigit Ozkan, B., & Spruit, M. (2023). Adaptable Security Maturity Assessment and Standardization for Digital SMEs. Journal of Computer Information Systems, 63(4), 965–987. 10.1080/08874417.2022.2119442