

RGA | Leaders of Tomorrow
An International Insurance Society Program

Insurance and Cyber Risk facing SMEs in Developing Economies from an Actuarial Lens

Olaoluwa Tolulope Olaopa
Head, Actuarial Services
Custodian Life Assurance

Contents

Abstract 3
Introduction 4
Digitization and digital transformation 4
Cyber Risk in Developing Economies 5
General Characteristics of SMEs 6
Cyber risk exposure of SMEs in developing economies resulting from digitization 7
An Actuarial Framework for Cyber Risk 9
Designing a Cyber Insurance Product for SMEs in a Developing Economy 11
Key Actuarial Challenges 12
Regulatory and Public Policy Considerations 13
Conclusion and Recommendations 13
References 15

Abstract

Small and medium-sized enterprises are vital to economic growth in developing economies. As more SMEs adopt digital tools and online channels, they also become increasingly exposed to cyber threats and attacks. However, many SMEs lack the resources, technical capacity, and financial protection needed to prevent cyber risks or recover from losses when incidents occur.

The Need to Close the Protection Gap

Cyber-related financial losses can threaten the survival of an SME, particularly where there is no adequate insurance or risk-transfer mechanism in place. If these businesses fail, the wider impact can be harmful to employment, productivity, and economic development.

To address this protection gap, greater attention should be given to cyber insurance solutions designed specifically for SMEs in developing countries. These products should be:

- Simple and accessible: easy to deploy, including through mobile phones or other digital channels.
- Efficient to underwrite: supported by straightforward onboarding and policy issuance processes.
- Affordable: priced in a way that reflects the financial realities of SMEs.
- Supported by the right environment: enabled by appropriate regulatory changes and broader economic development assistance.

The Role of Actuaries

Actuaries can play an important role in identifying emerging cyber risk trends and translating limited data into practical, relatable insights. By applying their technical expertise, actuaries can support the development of suitable and affordable cyber insurance products that help bridge the existing protection gap. In doing so, they can contribute to greater resilience among SMEs and provide a measure of stability when cyber incidents occur.

Introduction

The world has become increasingly digital, and technological advancement continues to accelerate the pace of global digitization. While digitization improves business processes and expands access to services, it also introduces significant risks. The growing reliance on computers, smart devices, and connected systems has increased exposure to cyber threats, including data breaches, targeted hacking, and other forms of cybercrime that can result in financial loss, reputational damage, and business disruption.

Small and medium enterprises (SMEs) which form a critical segment of the economy are major drivers of digitization globally and can be seen as easy targets for cyber criminals due to their relatively small size which may make them to be more vulnerable to cyber-attacks.

Meanwhile, Actuaries have long played an important role in managing uncertainty and risk. Although cyberspace is not a traditional actuarial practice area, technological growth affects all sectors, including the actuarial profession. Given their experience in risk management, product design, pricing, and reserving across different risk classes, actuaries can adapt their skills to assess and manage cyber risk in this emerging area.

Digitization and Digital Transformation

Digitization as broadly defined by the European Central Bank (2021), is defined as "including, inter alia, a wide range of information and communication technologies (ICT), technologies enabling automation and robotisation, and technologies related to the processing and analysis of digital data, including big data, such as artificial intelligence and machine learning, and edge and quantum computing".

This definition shows that digitization involves three interrelated elements: data, including its processing, transfer, and storage; technology; and human expertise.

Digital transformation is growing rapidly in developing economies. For instance, in 2025, Africa recorded over 1.1 billion mobile subscriptions and more than $1.1 trillion digital transactions (INTERPOL, 2026). Also, there are more than 570 million users who now depend on digital platforms for financial services, government access, healthcare and education in Africa (INTERPOL, 2026).

Although digitization could be generally seen as a positive change, since it creates value and has economic advantages, it has been found that globalisation, digitalisation and smart technologies have increased the tendencies and severity of cybercrime (Cremer et al, 2022). At the same time, in developing economies, the speed at which it is occurring is faster than the pace of the resources (cyber security infrastructure, regulatory framework and institutional capacity) needed to handle or manage it (INTERPOL, 2026). This creates a possible gap and increases the downside risk.

SMEs are important enablers of digital transformation (ENISA, 2021) and already form a core part of the wider economy. As a result, they play a significant role in the digitization process while also creating a channel through which cyber risks can increase.

Cyber Risk in Developing Economies

Cyber risks in developing economies are mainly driven by the rapid digitization, gaps in technical capacity and concentration of critical services. Also, the economic impact of cyber incidents is potentially more severe in developing nations, where estimates indicate that the average disclosed cyber incident has a larger impact than in developed nations (Vergara Cobos, 2024).

With the acceleration of the digital age globally, the world has been gripped by a series of cyber incidents that are increasing in both size and complexity. From 2014 to 2023, disclosed cyber incidents worldwide grew at an average annual rate of 21 percent (Vergara Cobos, 2024) and developing countries account for approximately 30 percent of the world's publicly disclosed cyber incidents (Vergara Cobos, 2024).

In a 2025 briefing, the World Bank Group said that "Developing countries are particularly vulnerable because they often lack the institutional capacity and technical know-how to effectively protect the data that fuels their digital transformation, including the personal data of their citizens". This indicates the huge gaps in the technical capacity of developing countries.

According to INTERPOL's 2026 report, the financial impact of reported cybercrime related losses in Africa rose from $192 million in 2024 to $484 million in 2025, while an aggregate estimate of $5 billion in direct economic damage from across the continent in 2025 resulted from cybercrime (INTERPOL, 2026).

Globally, cyber security breaches (such as ransomware, hacking and identity theft and Supply chain Exploitation) have increased over the years – by 40% in 2026, up by 18% in 2025 and a 70% increase since 2023 (SentinelOne, 2026).

Also, across west and Southern Africa, cybercrime accounts for over 30% of crimes in 2025 – up from between 10% - 30% in 2024 (INTERPOL, 2026), which reflects growing cyber incidence and concerns in those regions.

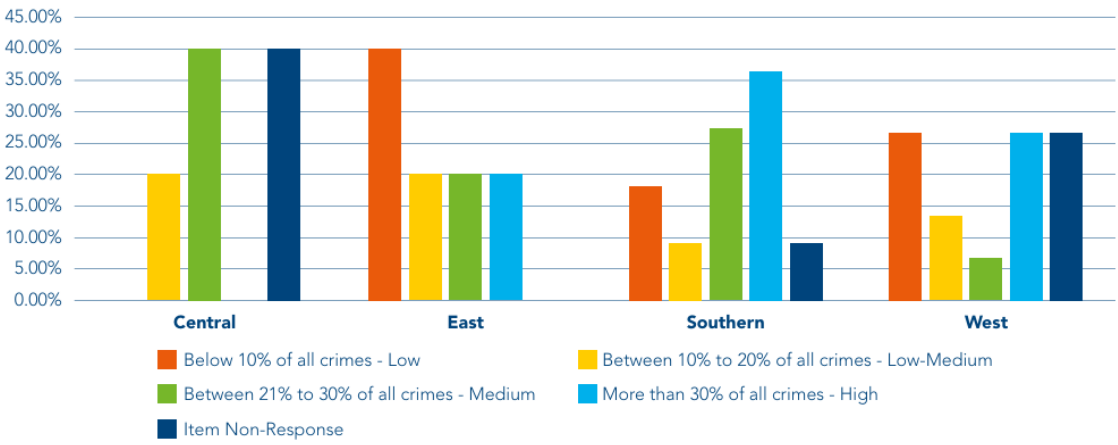

Figure 1: Perceived level of cybercrime as a percentage of all reported crime across Africa region-by-region in 2025 (Source: INTERPOL African cyberthreat assessment report 2026)

General Characteristics of SMEs

The European commission defines small and medium enterprises (SMEs) as a business with fewer than 250 employees and a turnover of less than or up to 50 million Euros. Also, according to the World bank, SMEs represent 90% of all businesses and they account for over half of global employment (World bank, 2026).

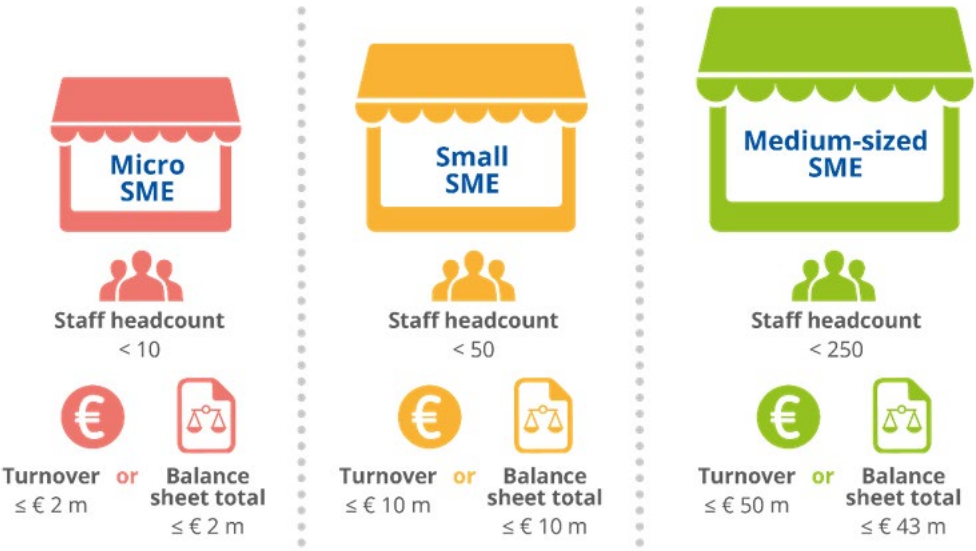

Figure 2: Characteristics of SMEs (Source: ENISA, cybersecurity for SMES 2021)

This clearly shows that a lot of businesses can be classified as SMEs. Therefore, SMEs play a critical role in economic development (Adriko and Nurse, 2024) and in developing economies, they are central to economic diversification and productivity (World bank, 2026).

When considering cyber risk, SMEs are particularly vulnerable because their smaller size and limited financial capacity may prevent them from implementing adequate preventive measures and security tools. These constraints can make them easier targets for cyber criminals.

Also, so many SMEs, due to their size, deal with retail customers and in some instances, they act as a bridge between an individual customer and larger businesses. As a result of this, the cyber risk faced by SMEs has the potential to accumulate into a bigger risk, and they could also be the weak link in the cyber security structure of larger organizations.

This challenge is more pronounced in developing economies, where inadequate infrastructure, limited expertise, and constrained resources can increase SMEs' vulnerability and exposure to cyber risks.

Cyber risk exposure of SMEs in developing economies resulting from digitization

SMEs in developing economies are rapidly adopting technology as a way of reducing costs and scaling up. However, most developing economies do not have adequate cyber infrastructure and regulations that can help reducepotential risk exposures.

The main cyber risks facing SMEs include data and confidentiality breaches, service disruption, system integrity failures, and online fraud. These risks may arise from one event or a combination of events, including phishing, business email compromise, login credential theft, data breaches, malware or ransomware attacks, distributed denial-of-service attacks (DDoS), and payment diversion (ENISA, 2021; INTERPOL, 2026).

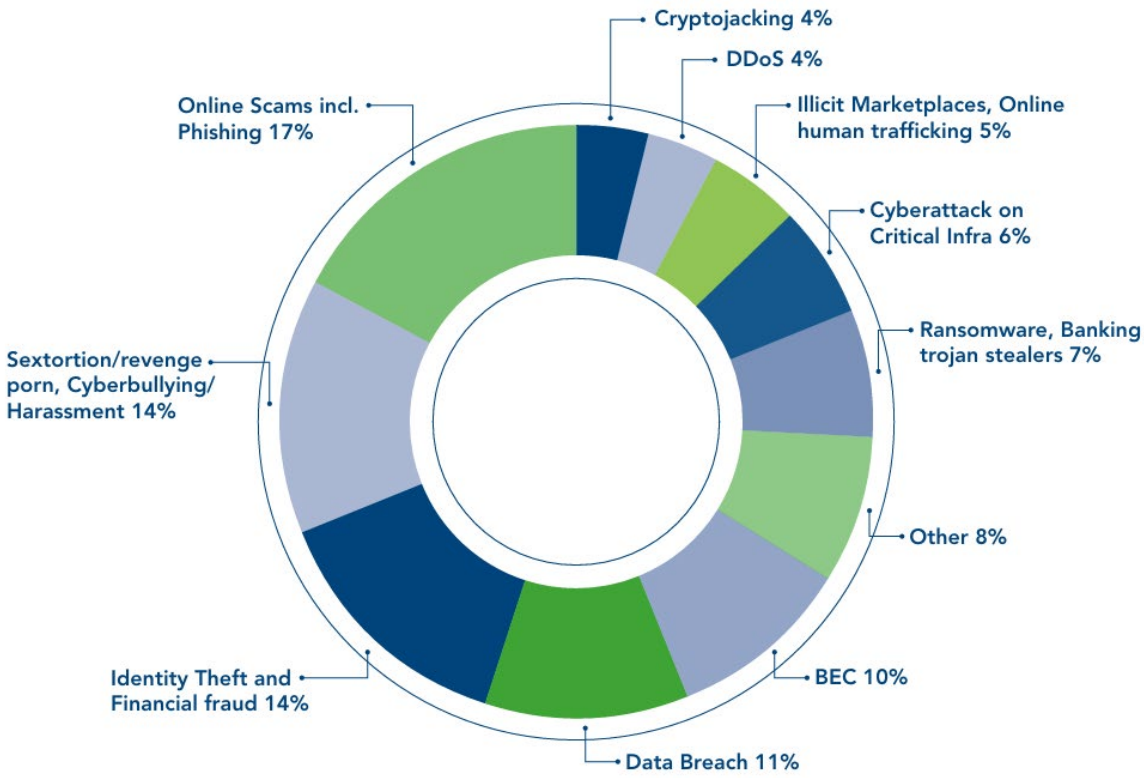

Figure 3: Reported Cybercrime cases in Africa by type in 2025 (Source: INTERPOL African cyberthreat assessment report 2026)

In 2021, ENISA identified ransomware, stolen laptops, phishing and chief executive officer fraud are among the most common incidents affecting SMEs. It was also reported that 90% of surveyed SMEs expected serious negative impact within one week of a cybersecurity issue, while 57% considered bankruptcy or closure likely after a serious incident (ENISA, 2021).

In recent times, mobile money payment, point-of-sale terminals, e-commerce platforms, telemedicine, remote working, digital payrolls, cloud accounting systems, digital customer relationship tools and outsourced technology providers are rapidly becoming common in the SMEs segment of developing economies. This implies that sensitive and confidential private business or customer data are being transmitted, transferred and stored digitally through applications, systems and networks.

This increase in online presence has increased the risk of becoming a victim of phishing attacks, identity theft and other forms of social engineering by cyber criminals, and this could lead to significant financial loss for victims.



Figure 4: Characteristics of SMEs (Source: ENISA, cybersecurity for SMES 2021)

Many businesses, including SMEs, in developing economies are moving from paper-based operations and physical data storage to digital databases and cloud-based storage. This shift exposes them to cyber risks such as network disruption, data breaches, system and database compromise, and ransomware attacks by malicious actors.

There have also been incidents of inability to access critical systems or denial of service attacks and other forms of connectivity or network issues. This can result in significant business disruption, operational loss and loss of business income depending on the scale and level of business dependence. For example, a faulty update by CrowdStrike, a cybersecurity service provider, in 2024 led to a widespread disruption of millions of systems globally (Munich Re, 2025). It has been confirmed that it was not a malicious attack, but this resulted in one of the largest IT outages ever recorded that affected key and critical industries and sectors like airline and airports, financial services, technology and healthcare services (Munich Re, 2025).

Another significant cybersecurity challenge for SMEs in emerging economies is the shortage of cybersecurity professionals. Where skilled expertise is unavailable or inadequate, systems may remain exposed or insufficiently protected against cyber threats and attacks. This can ultimately result in serious financial losses for the business.

Where breaches from any of these possible forms occur, there could be business disruption, data theft, regulatory sanctions, litigation, reputational damage and other forms of financial losses which could be significant.

Many SMEs in developing economies face a significant protection gap. They often lack adequate cyber-risk protection, the technical capacity to reduce their exposure, and the financial resources required to restore operations after a cyber incident. This creates an important opportunity for actuaries to support the market by designing cyber insurance products that are simple, affordable, and tailored to the needs of SMEs.

An Actuarial Framework for Cyber Risk

The basic concept of insurable risk provides a useful starting point. A risk is generally considered insurable where it has low frequency and high severity. In other words, the probability of loss is relatively low, but the financial impact can be significant if the insured event occurs.

Cyber risk can therefore be viewed as an insurable risk. The financial impact of a realized cyber event is often high, while the frequency of occurrence is typically lower. However, as gaps in protection and preventive controls widen, the frequency of cyber risk events may continue to increase. This makes cyber risk an area in which actuarial expertise is highly relevant.

Now considering the case of SMEs of a developing economy, the severity of cyber events would be high while the frequency is expected to remain low although it may be slightly higher than those of developed economies because of the gaps in protection and infrastructure.

So, for an SME of a developing economy, the key drivers of loss frequency could be industry/market segment, business size, level of employee training, internet exposure, digital footprint, payment channels, payment volume, software patching, use of cloud providers, level of security control and cyber protection available.

On the other hand, loss severity is determined by factors such as size of breach, forensic costs, legal expenses, notification costs, regulatory fines, ransom payments, system restoration, business interruption, reputational loss and third-party liability.

We would also expect that there may be aggregation of losses on the portfolio since several similar businesses may be involved although the probability of this may be relatively low.

Therefore, we can make use of an individual or collective risk model to estimate the aggregate loss at the portfolio level, while a copula is used to estimate the joint probability of dependent losses.

Jevtic and Lanchier (2020) proposed a structural model of aggregate loss distribution for cyber risk of SMEs under the assumption of a tree-based LAN topology.

The aggregate loss is the sum of individual losses over a known period. In actuarial notation, if N is the random variable representing the number of cyber incidents and X is the random variable which represents the claims amount for each incident, then the aggregate loss, S can be expressed as:

$$S = X_1 + X_2 + \cdots + X_N$$

While a copula which is simply defined as a function that expresses a multiple cumulative distribution function (CDF) in terms of its individual marginal CDFs, can be used to estimate the probability of multiple or aggregate losses.

So, we are basically using the joint distribution of multiple univariate distributions to estimate the probability of the aggregate loss.

$$C(u_1 + u_2 + \cdots + u_N) = F_{X_1+X_2+\cdots+X_N}(X_1 + X_2 + \cdots + X_N)$$

Where $u_i = F_{X_i}(X_i)$ is the marginal cumulative distribution function of the individual claim amount random variable and *C* is the copula function.

Copulas can further be used to assess the dependence of individual losses (Eling and Jung, 2018) since losses tend to occur together.

The coefficient of upper tail dependence would give us an indication of whether high values of one loss random variable, X tends to be linked with high values of another loss random variable Y. While the coefficient of lower tail dependence would give us an indication of whether low values of one loss random variable, X tends to be linked with low values of another loss random variable Y.

In the case of SMEs cyber risk events, we expect to see some form of relationships between different losses. So, the coefficient of tail dependence would help with some modeling decisions.

Designing a Cyber Insurance Product for SMEs in a Developing Economy

A suitable cyber insurance product for SMEs in developing economies should have two main characteristics:

- Simplicity and
- Affordability.

Adriko and Nurse (2024) found out that may SMEs do not prioritize cyber insurance for reasons which include concern about the cost, limited awareness and minimal value if not required by clients or regulators.

It is therefore important that cyber insurance policies designed for SMEs in developing economies are simple and affordable. Simplicity may imply limited coverage, but the product should still address core cyber risks and provide meaningful protection for SMEs. Just like third-party motor insurance, which offers basic protection at a lower price than comprehensive motor insurance, insurers and actuaries should consider a tiered approach that balances affordability with essential coverage.

Examples of possible coverage provided by a basic policy include incident response costs, data restoration, business interruption, cyber extortion response, payment of fraud support, and third-party liability.

Policy wording and conditions should also be written in simple terms that would leave no room for ambiguity, and client onboarding should be as seamless as possible.

It is also important that a cyber insurance product for SMEs in emerging economies is affordable especially because most of them operate on tight budgets and may already

have slim profit margins, hence they may see little benefit in paying large sums at the expense of their business profitability and survival if the premiums are expensive.

Product simplicity and affordability would ensure that adequate cover is achievable for SMEs, and it would foster trust and confidence in the insurer.

Key Actuarial Challenges

The key challenges are:

- Data
- Moral hazard
- Anti-selection

Data availability and credibility have been the main challenges for assessing cyber risk. It has been noted that despite the increasing importance for the global economy, the availability of data on cyber risks remains limited (Cremer et al, 2022). Historical data is not readily available due to under reporting and regulatory gaps in developing economies. It has been established that organizations generally are unwilling to reveal details of cyber incidents (Rong He et al, 2024). This has immensely contributed to the lack of adequate data.

For SMEs in emerging economies, data availability is even worse especially because of the unstructured mode of operation and because they may prefer not to report cyber incidence because of the reputational risk and potential financial consequences like penalties or fines from regulators and legal cost.

Actuaries need data, especially actual insurance claims data to develop models (Rong He et al, 2024) and price cyber risk appropriately. In the absence of adequate data, parameter estimates become unreliable, and cyber insurance products may become unnecessarily expensive.

A further challenge is that some SMEs may become less disciplined about cybersecurity controls after purchasing cyber insurance. Moral hazard is a common issue in insurance and can increase the cost of coverage. In this context, SMEs may underinvest in adequate controls. This risk can be mitigated through policy excesses and premium discounts for businesses that maintain strong cyber controls.

Lastly, SMEs with weak or vulnerable controls may be more likely to buy a cyber insurance product. This tendency, which is known as anti-selection, can be mitigated by ensuring proper underwriting, advocating for proper cyber security practice, price differentiation and training campaign for SMEs staff.

Regulatory and Public Policy Considerations

Regulatory and infrastructure gaps in cybersecurity across developing economies must be addressed urgently. If these gaps remain, malicious actors will have greater opportunities to exploit vulnerabilities, which could result in severe financial and economic consequences for businesses of all sizes.

Sustainable economic growth depends on protecting the basic digital infrastructure on which businesses operate. Governments and regulators therefore need to establish clear cybersecurity requirements, including data protection rules, incident-reporting obligations, and minimum security-control standards for businesses. They should also support continuous awareness campaigns, enforce compliance with applicable laws, and encourage the training and upskilling of cybersecurity professionals who can help reduce exposures and manage emerging cyber risks.

A public cyber risk database could also be created so that adequate data is readily available for purposes such as pricing or risk modelling.

Conclusion and Recommendations

- SMEs which are the backbone of economic growth in developing economies are increasingly going digital, and this increasing digital footprint increases their vulnerability to potential cyber threats.
- SMEs in developing economies are exposed to cyber risk because of lack of protection and technical know-how and since any successful cyber-attack could have severe financial impact, there is a need to provide an affordable cyber insurance cover for them.
- Actuaries who have traditionally been involved in risk management and insurance product development and pricing, can use tools such as aggregate risk models and copulas to model the severity and likelihood of potential cyber events. This could help cushion the financial burden that can result from cyber-attacks.
- There is a need for stronger cybersecurity infrastructure and regulatory supervision across the SME segment in developing economies. Regulators should consider minimum cyber-protection requirements as part of business licensing and licence renewal process, like the minimum solvency of capital requirements in certain regulated sectors.
- Continuous awareness and training should be provided for SME employees. Staff should be trained to identify, prevent, and respond to cyber threats, as well as to reduce the organisation's exposure to evolving risks. In addition, developing economies should invest in training more cybersecurity professionals to strengthen local capacity and improve their ability to respond to cyber incidents effectively.

- Incident reporting should be encouraged, and from this reporting, a public database could be developed allowing transparency of learning and accountability. This would also help actuaries design solutions that are better suited to SMEs in developing economies.

References

- Adriko, R., & Nurse, J. R. C. (2024). Cybersecurity, cyber insurance and small-to-medium-sized enterprises: A systematic review. Information and Computer Security, 32(5), 691–710. https://doi.org/10.1108/ICS-01-2024-0025

1. Cremer F., Sheehan B., Fortmann M., Kia A., Mullins M., Murphy F., Materne S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice (2022) 47:698–736
2. Eling, M., and K. Jung (2018). Copula approaches for modeling cross-sectional dependence of data breach losses. Insurance Mathematics & Economics 82: 167–180. https://doi.org/10.1016/j.insmatheco. 2018. 07. 003.
3. ENISA. (2021). Cybersecurity for SMEs: Challenges and Recommendations. European Union Agency for Cybersecurity.
4. European Central Bank (2021). "Digitalisation: Channels, Impacts and Implications for Monetary Policy in the Euro Area." European Central Bank Occasional Paper Series No. 266.
5. European Commission. (2026). SME definition.

   https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en (Accessed: 5th August 2026).
6. INTERPOL (2026). INTERPOL African Cyberthreat Assessment Report 2026.

   https://www.interpol.int/Media/Documents/Publications/Cybercrime/African-Cyberthreat-Assessment-Report-2026 (Accessed: 5th August 2026.)
7. Jevtic P, Lanchier N (2020) Dynamic structural percolation model of loss distribution for syber risk for small and medium-sized enterprises for tree based LAN topology. Insur Math Econ 91:200 – 233.
8. Munich Re. (2025). Cyber insurance: Risks and trends 2025. Munich Re

   https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html
9. Rong H., Zhuo J., and Johnny S. (2024). Modeling and Management of cyber risk: a cross-disciplinary review. Annals of Actuarial Science (2024), 18, pp. 270 – 309.
10. SentinelOne (2026). Key Cyber Security Statistics for 2026.

    https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

11. Vergara Cobos (2024). Cybersecurity economics for emerging markets. World Bank group.

    https:// openknowledge.worldbank.org/

12. World Bank Group (2025). Enhancing Cyber Resilience in Developing Countries.

    https://www.worldbank.org/en/results/2025/01/29/enhancing-cyber-resilience-in-developing-countries

13. World Bank. (2026). SME finance. https://www.worldbank.org/ext/en/topic/competitiveness/small-and-medium-enterprises-smes-finance (Accessed: 5th August 2026).