مجلة البحوث الإدارية والمالية والكمية

Journal of Managerial, Financial & Quantitative Research

جامعة السويس
كلية التجارة

Cyber Insurance Pricing Through Monte Carlo Simulation: A Case Study of the Egyptian Insurance Market

Submitted by

Sayed Mohamed Gouda

Assistant Professor

Quantitative Sciences Department

Faculty of Commerce - Suez University

M.Sc. in Insurance – Cairo University

Ph.D. in Insurance – McMaster University (Canada) & Cairo University

CRM Designation, CRMP Fellow

Islam Farid Mostafa

Assistant Professor

Insurance & Actuarial Science Department

Faculty of Commerce - Cairo University

Journal of Managerial, Financial and Quantitative Research
Faculty of Commerce – Suez University
Vol. 5 No. 3 September 2025

Website: https://safq.journals.ekb.eg/

Cyber Insurance Pricing Through Monte Carlo Simulation: A Case Study of the Egyptian Insurance Market

Abstract:

This study introduces a dual-model approach to pricing cyber risk insurance, specifically designed for Egypt's insurance market, utilizing Monte Carlo simulation methods. The first model uses a probabilistic risk-based pricing framework, simulating claim costs under optimistic, moderate, and pessimistic scenarios with normally distributed loss values. Premiums are set by applying risk-adjusted multipliers to the average projected losses, helping ensure both profitability and adequate capital reserves. The second model focuses on annual cyber losses, combining Poisson-distributed attack frequencies with normally distributed loss severities to estimate yearly losses across five types of organizations: Low Risk, Moderate Risk, High Risk, Tech Firms (with high severity), and Retail Chains (with high frequency). Through 10,000 iterations per scenario, the study calculates key financial measures, including expected profits, loss probabilities, and five-year Net Present Values (NPVs). Findings reveal that while some sectors show stable profitability, others—particularly tech firms—face high chances of losses and negative NPVs, indicating potential underpricing. The research highlights the value of using scenario-based stochastic models, deductible options, and confidence intervals to enhance underwriting precision and portfolio resilience. The study concludes by recommending that Egyptian insurers adopt data-driven, risk-sensitive pricing strategies that factor in both loss frequency and severity, along with maintaining capital buffers to manage the volatility inherent in cyber risk effectively.

Keywords: Cyber Insurance, Monte Carlo Simulation, Risk-Based Pricing, Egyptian Insurance Market, Cyber Risk

ملخص البحث

تقدم هذه الدراسة نهجًا ثنائي النموذج لتسعير التأمين ضد مخاطر الإنترنت، صُمم خصيصًا لسوق التأمين المصري، باستخدام أساليب المحاكاة مونت كارلو .يعتمد النموذج الأول على إطار تسعير احتمالي قائم على المخاطر، حيث تتم محاكاة تكاليف المطالبات في سيناريوهات متفائلة ومعتدلة ومتشددة مع افتراض التوزيع الطبيعي لقيم الخسائر. ويتم تحديد الأقساط عبر تطبيق معاملات معدلة حسب المخاطر على متوسط الخسائر المتوقعة، مما يساهم في ضمان كل من الربحية وتوافر الاحتياطيات الرأسمالية الكافية.

أما النموذج الثاني فيركز على الخسائر السنوية الناتجة عن الهجمات الإلكترونية، من خلال الجمع بين توزيع بواسون لتكرار الهجمات والتوزيع الطبيعي لشدة الخسائر، وذلك لتقدير الخسائر السنوية عبر خمسة أنواع من المؤسسات: منخفضة المخاطر، معتدلة المخاطر، عالية المخاطر، شركات التكنولوجيا (بشدة خسائر مرتفعة)، وسلاسل التجزئة (بارتفاع تكرار الهجمات). ومن خلال 10,000 تكرار لكل سيناريو، تحسب الدراسة مؤشرات مالية أساسية تشمل الأرباح المتوقعة، احتمالات الخسارة، وصافي القيمة الحالية (NPV) لخمس سنوات.

تكشف النتائج أن بعض القطاعات تُظهر ربحية مستقرة، بينما تواجه أخرى – وخاصة شركات التكنولوجيا – احتمالات عالية للخسائر وصافي قيمة حالية سلبي، مما يشير إلى احتمال تسعير غير كافٍ. وتبرز الدراسة أهمية استخدام نماذج عشوائية قائمة على السيناريوهات، وخيارات التحمل(Deductibles) ، وفترات الثقة لتحسين دقة الاكتتاب وتعزيز مرونة المحفظة.

وتخلص الدراسة إلى التوصية بأن يتبنى الممارسون في سوق التأمين المصري استراتيجيات تسعير قائمة على البيانات وحساسة للمخاطر، تأخذ في الاعتبار كلًّا من تكرار وشدة الخسائر، إلى جانب الحفاظ على احتياطيات رأسمالية لمواجهة التقلبات المتأصلة في المخاطر السيبرانية.

الكلمات المفتاحية :التأمين السيبراني، محاكاة مونت كارلو، التسعير القائم على المخاطر، سوق التأمين المصري، المخاطر السيبرانية.

1. Introduction

In today's digital age, cyberattacks are becoming more frequent and severe, creating significant financial and operational challenges for organizations of all sizes. As reliance on digital systems increases, so does the global demand for cyber insurance—and Egypt is experiencing this trend as well. However, the complexity of cyber threats and the limited historical data available in emerging markets make traditional actuarial methods inadequate for setting fair and sustainable premiums.

To address this issue, the study explores two quantitative methods specifically designed for Egypt's insurance market. The first method employs a probabilistic risk modelling framework with Monte Carlo simulations to estimate premiums under various threat scenarios—optimistic, moderate, and pessimistic—based on expected claim costs and their variability. The second method models annual cyber losses by integrating Poisson and normal distributions to illustrate both the frequency of attacks and their potential financial severity across different types of organizations.

By combining these simulation techniques, insurers can better measure uncertainty, estimate potential losses, evaluate profitability, and set premiums that reflect diverse risk levels. This research illustrates how such models can be effectively applied in the Egyptian context, offering data-driven guidance and recommendations for developing sustainable and competitive cyber insurance pricing strategies.

2. Research Problem

As cyber threats continue to grow in both frequency and complexity—and as organizations become increasingly dependent on digital infrastructure—cyber insurance has emerged as a critical component of modern risk management. However, insurers in Egypt face significant obstacles in accurately pricing these policies. Among the key challenges are a shortage of local historical data on cyber incidents, the constantly evolving nature of cyber threats, and the lack of advanced actuarial or simulation-based pricing models specifically designed for Egypt's unique risk environment.

The Kaspersky META 2025 Cyber Threat Report brings these issues into sharper focus. It ranks Egypt among the most heavily targeted countries in the region, citing a notable rise in ransomware attacks and sophisticated cyber-espionage operations, including campaigns like SideWinder (Abbast, 2025). These threats are becoming more advanced, targeting critical sectors such as government, telecommunications, and finance. The report highlights the lack of preparedness among many insurers in assessing and pricing cyber risk in this dynamic landscape.

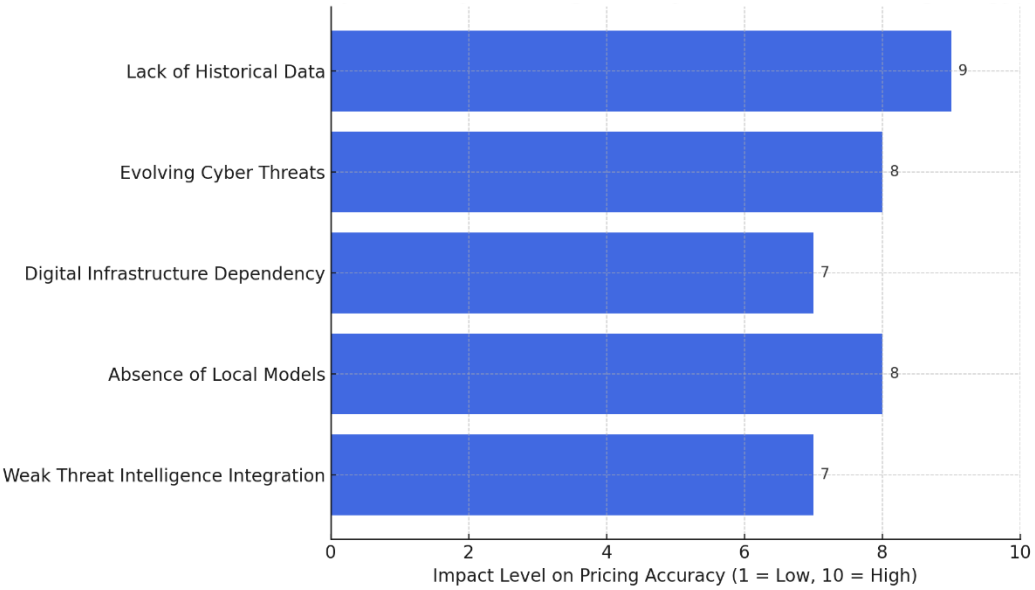
A recent real-world example illustrates the stakes. In 2025, a fire at the Ramsis Central in Cairo quickly turned into a digital crisis, disrupting internet and mobile services across the country. Though it began as a physical incident, it revealed just how deeply intertwined physical and cyber systems have become. It also exposed serious shortcomings in how such hybrid risks are evaluated, covered, and priced within Egypt's insurance market.

Traditional insurance pricing models, while effective for more predictable types of coverage, often fall short when applied to cyber risks. These risks are harder to quantify, can cause widespread disruption,

and frequently involve complex chain reactions. This raises a pressing question: What can Egyptian insurers do to build smarter, more reliable pricing models for cyber insurance that account for both the frequency and severity of losses in such a volatile environment?

One promising path forward involves the use of Monte Carlo simulations and probabilistic risk modelling. These tools enable insurers to explore a wide range of possible outcomes, assess risk-adjusted profitability, and set premiums that more accurately reflect the true level of exposure. Incorporating regional threat intelligence, such as insights from the Kaspersky report, can further improve these models by grounding them in real-world data about attack patterns, target sectors, and emerging risks.

Figure (1): Impact of Key Challenges on Cyber Insurance Pricing in Egypt



The impact scores (1–10) shown in the chart are qualitative estimates derived from authoritative sources such as the Kaspersky META 2025 Cyber Threat Report and Biener, Eling, and Wirfs (2015), offering insight into key challenges affecting insurers' ability to model and price cyber risk—particularly in emerging markets like Egypt. The most critical issue, rated 9, is the lack of historical local data, which hampers actuarial accuracy and risk-based pricing. The evolving nature of cyber threats, scored at 8, reflects how fast-changing malware and advanced persistent threats (APTs) undermine traditional models. A score of 7 is assigned to systemic risks arising from digital interdependence, as seen in hybrid incidents like the Ramsis fire, which exposed blind spots in current pricing strategies. Additionally, the use of imported, non-localized models (score: 8) fails to reflect Egypt's unique cyber landscape, while poor integration of regional threat intelligence (score: 7) further weakens underwriting precision. These factors highlight the urgent need for localized, adaptive modelling approaches in cyber risk insurance.

2.1.Significance of the Research

This research is important because it advances the way cyber insurance is priced within Egypt's insurance sector. As cyber threats grow more frequent and complex, Egyptian insurers urgently need more advanced tools for assessing risk and setting premiums. At present, many insurers in Egypt either avoid cyber insurance altogether or rely on foreign pricing models that don't fully capture local market conditions. This study fills that gap by creating a data-driven, locally tailored pricing model using Monte Carlo simulation techniques.

By employing probabilistic modelling, the research offers a systematic method to estimate annual losses, expected profits, and premium strategies for different cyber risk profiles. These moves are underwriting away from intuition and experience-based decisions toward a more evidence-based approach, allowing insurers to price policies according to actual risk exposure. The inclusion of actuarial elements like deductibles, loss probability distributions, and net present value (NPV) calculations ensures the pricing model remains competitive while being financially sustainable over time.

The study also supports the broader development of Egypt's cyber insurance market. By providing transparent, actuarially sound premiums, insurers can build trust with corporate clients—particularly small and medium-sized enterprises (SMEs), which are highly vulnerable to cyberattacks yet often uninsured. This contributes to strengthening Egypt's digital economy and improving the nation's overall cyber risk management capabilities.

Furthermore, the findings carry strategic and regulatory significance. They can guide insurers in product design, risk segmentation, and reinsurance decisions, while also offering valuable input for policymakers and regulators like the Egyptian Financial Regulatory Authority (FRA) in setting national cyber insurance pricing standards. Overall, this research establishes a solid foundation for further cyber risk modelling studies, not just in Egypt but in other emerging markets facing similar challenges.

2.2.Research Objective

The main goal of this research is to create a strong and locally relevant cyber insurance pricing model specifically designed for the Egyptian insurance market, utilizing Monte Carlo simulation techniques. The study focuses on simulating annual cyber loss scenarios for a range of organizational risk profiles—from low-risk companies to those facing frequent or severe attacks—by combining probabilistic modelling of both attack frequency and loss severity. The objective is to estimate expected yearly losses, assess insurer profitability, and set actuarially fair premiums. Additionally, the research incorporates important actuarial elements like deductible structures, confidence intervals, and multi-year Net Present Value (NPV) analyses to improve the accuracy and long-term financial stability of the pricing model. Ultimately, this approach aims to enable Egyptian insurers to make informed, data-

driven underwriting decisions and contribute to the development of a more resilient and transparent cyber insurance market.

2.3.Research Hypotheses

- H1: A simulation-based pricing model will yield premiums that align more closely with the actual risk exposure compared to traditional fixed-rate pricing methods.
- H2: The incorporation of deductibles and NPV analysis over multi-year periods will enhance the model's ability to project profitability and manage long-term underwriting risk.

Testing these hypotheses through scenario-based simulations will provide insights into how well the model performs and how it can be adapted to local market dynamics in Egypt.

2.4.Scope of the Research

This study aims to develop a simulation-based cyber insurance pricing model specifically designed for the Egyptian insurance market. Using Monte Carlo simulation, it estimates annual cyber losses, calculates risk-based premiums, and assesses Net Present Value (NPV) over a five-year timeframe. The model covers five organizational risk profiles, ranging from low-risk entities to those facing high-frequency or high-severity cyber threats. It incorporates probabilistic distributions such as Poisson and Normal, along with deductibles and confidence intervals. However, the study has some limitations. Real historical cyber claims data from Egyptian insurers were unavailable, so the model relied on synthetic data derived from global trends and expert input.

2.5.Related Literature

In recent years, there has been an increasing amount of research focused on cyber insurance pricing and modelling, reflecting the growing sophistication and frequency of cyber threats across various industries. Researchers like Biener, Eling, and Wirfs (2015) highlight the need for actuarial and risk-based pricing approaches to establish sustainable cyber insurance markets, especially in emerging economies. Traditional pricing methods, which depend largely on historical claims data and fixed assumptions, are now being complemented by probabilistic techniques such as Monte Carlo simulations, due to the unpredictable and rapidly changing nature of cyber risks.

Monte Carlo simulations have become particularly valuable for capturing complex risk profiles, allowing insurers to run thousands of simulations that model random variations in both the frequency and severity of cyber incidents (Herzog, 2011). For example, Romanosky et al. (2019) demonstrate how stochastic models improve the understanding of extreme loss events and the risk of insurer insolvency from catastrophic cyber-attacks. Likewise, Maillart and Sornette (2010) emphasize the importance of heavy-tailed distributions to realistically represent rare but severe cyber losses that significantly impact pricing decisions.

However, research specific to cyber insurance in the MENA region, and Egypt in particular, remains limited. With the rapid digital transformation of Egyptian businesses, there is a pressing need for pricing tools tailored to local conditions. Previous work on Egypt's insurance market (e.g., Abdelmottaleb & Soliman, 2020) stresses the necessity for innovative pricing and underwriting methods to address emerging, intangible risks. This study builds on that foundation by proposing a simulation-based pricing model designed to fit Egypt's unique cyber risk environment.

Overall, this research connects advanced international modelling techniques with the practical needs of the Egyptian insurance sector, contributing to both academic understanding and the real-world application of cyber risk management in developing insurance markets.

Aligned with this growing literature, Awiszus et al. (2023) explore cyber insurance pricing by incorporating different layers of risk—idiosyncratic, systematic, and systemic—highlighting the interconnected nature of cyber events. Skeoch and Pym (2023) examine cyber insurance from a socioeconomic perspective, using maturity models to study how organizational behaviour influences coverage decisions. Antonio, Indratno, and Saputro (2021) present a Markov-based dynamic model that uses clustering techniques to improve premium calculations under varying conditions. From a market perspective, Böhme (2005) discusses the challenges posed by correlated cyber risks, which complicate risk pooling and weaken traditional insurance frameworks. More recently, Ioannidis and Skeoch (2024) used Monte Carlo simulations to show how market inefficiencies arise from limited data sharing and insufficient reinsurance support. Hua and Xu (2020) contribute a flexible pricing framework based on synthetic data and a risk-spreading algorithm, demonstrated through a case study involving large-scale cyber networks.

3. Understanding Cyber Risks

3.1. Definition and Classification of Cyber Risks:

- **Cyber Risks**

Refer to the potential for harm or loss arising from the use of technology and digital systems, including the internet, to carry out activities such as online communication, financial transactions, or business operations. These risks are typically associated with various forms of cyber threats, vulnerabilities, and attacks that may compromise the security, confidentiality, or integrity of digital data, systems, and networks.

- **Classification of Cyber Risks**

Cyber risks can be categorized into several groups based on the nature of the threat, its potential impact, and the target. According to the OECD (2017), these risks include:

1. **Cybersecurity Threats:** This category covers direct threats to digital systems and data security, such as:

- **Malware**, including viruses, ransomware, spyware, and worms, which can damage systems or steal sensitive information.
- **Phishing and social engineering attacks**, where attackers trick individuals into revealing confidential data by posing as legitimate sources.
- **Denial-of-Service (DoS) attacks** flood networks or systems with traffic to make them unavailable to users.
- **Insider threats**, involving employees or contractors who, intentionally or not, cause data leaks or harm systems.
- **Data breaches**, when unauthorized parties gain access to protected information.
- **Ransomware**, which locks systems or data and demands payment to restore access, often in cryptocurrency.
- **Intellectual property theft** involves the unauthorized acquisition of valuable business information, like trade secrets or patents.
- **Third-party vulnerabilities**, which arise from weak cybersecurity practices among vendors, cloud providers, or partners.

2. **Operational Risks:** These are threats that disrupt business operations, including:
   - **System failures** due to hardware or software issues halt services.
   - **Supply chain disruptions** caused by cyber incidents affecting external vendors.
   - **Business interruptions** resulting from incidents like data loss or ransomware prevent normal operations.

3. **Financial Risks:** These risks have a direct monetary impact, such as:
   - **Fraud**, including identity theft, fake transactions, or credit card scams.
   - **Economic losses** due to the theft of IP, customer data, or brand reputation damage, all of which can affect revenue.

4. **Legal and Compliance Risks:** Organizations may face consequences if they fail to comply with legal or regulatory standards:
   - **Regulatory violations**, such as breaching GDPR or other data protection laws, can lead to fines or legal action.
   - **Litigation**, which might come from customers, employees, or partners affected by data breaches or cyber incidents.

5. **Reputational Risks:** Cyber events can also affect public perception:
   - **Brand damage**, when trust is lost due to security failures.
   - **Public relations issues**, where the organization struggles to manage communication and stakeholder expectations after a breach.

6. **Strategic Risks:** These include long-term consequences, such as:
   - **Loss of intellectual property**, which may result from cyber espionage or hacking by competitors.
   - **Competitive disadvantage**, if innovations or strategic information are compromised, harming market performance.

7. **Privacy Risks:** This involves the mishandling or unauthorized access of personal data:

- **Unauthorized data access**, where sensitive personal or financial details are exposed.
- **Invasion of privacy**, when individuals' information is misused, sold, or shared without consent.

Figure (2): Estimated Distribution of Cyber Risk Types (Global Approximation)

This pie chart shows the estimated global breakdown of cyber risk types. Cybersecurity threats lead at 35%, followed by operational risks (15%) and financial risks (12%). Legal and compliance risks, strategic risks, and privacy risks each account for 10%, while reputational risks make up the remaining 8%. This distribution underscores the need for insurers to consider a broad spectrum of risk exposures—not just technical breaches—when pricing cyber insurance policies (OECD, 2022a).

3.2. Impacts of Cyber Risks

Cyber risks can cause extensive financial and operational harm to both organizations and individuals. These effects are often wide-ranging—spanning immediate monetary losses, long-term damage to reputation, and significant disruptions to day-to-day operations. The scale and severity of the impact largely depend on the type of cyber threat, the preparedness of the target, and how quickly and effectively the response is executed.

Financial Impacts

One of the most immediate consequences of cyberattacks is direct financial loss. Incidents such as ransomware, data breaches, and fraud can result in companies being forced to pay ransoms or absorb unauthorized transactions, leading to substantial financial setbacks (Böhme & Schwartz, 2010). Individuals are also vulnerable, falling victim to phishing schemes or malware attacks that can drain personal bank accounts or compromise sensitive financial data.

Table (1): Cyber Risk Financial Losses Report (Canada, South Africa, Saudi Arabia, Egypt)

Country	Annual Loss (USD)	Source
Canada	$3.82 billion	Statista (2023)
South Africa	$118 million	TechCabal (2025)
Saudi Arabia	~$8 million per breach	DW / IBM Study (2023)

Source: Canadian Centre for Cyber Security (CCCS) – cyber.gc.ca, South African Cybersecurity Hub – csirt.gov.za, National Cybersecurity Authority (Saudi Arabia) – ncsc.gov.sa, Egyptian National Telecom Regulatory Authority (TRA) – tra.gov.eg

This table illustrates the diverse impact of cybercrime across different countries. Canada reports the highest estimated annual loss at $3.82 billion, reflective of its highly digitized economy. South Africa, despite a smaller economy, still experiences significant losses, signalling growing cyber threats amid relatively low insurance uptake. Saudi Arabia's data presents a per-breach estimate, averaging $8 million per incident, highlighting the intensity of individual attacks on high-value targets. In contrast, Egypt lacks publicly available data, which underscores a critical gap in national reporting and transparency. This absence hinders insurers' ability to price cyber policies accurately and develop effective mitigation strategies. Establishing a national cyber incident reporting framework in Egypt could greatly support the development of its cyber insurance market.

Beyond direct financial losses, companies may face heavy regulatory fines for failing to protect sensitive data, especially under international laws such as the GDPR in Europe or HIPAA in the U.S. (Eling & Schnell, 2016). While individuals typically aren't fined, they may suffer legal and financial consequences if their data is exposed or misused.

The cost of recovering from a cyberattack can also be considerable. Businesses must often invest in cybersecurity experts, forensic audits, crisis communication, and upgrades to internal systems to restore operations and protect against future threats (OECD, 2017). On a personal level, affected individuals may need to subscribe to identity protection services or monitor their financial accounts to mitigate long-term damage.

Cyberattacks can also lead to a drop in business revenue, particularly for companies that rely heavily on digital services. E-commerce platforms and service-based industries are especially vulnerable to loss of income when operations are interrupted (Biener, Eling, & Wirfs, 2015). Likewise, individuals may lose earnings if the digital tools or platforms they depend on are compromised.

Another major financial consequence is reputational harm. A publicized data breach can damage customer trust and tarnish a company's image, often requiring significant time and investment to repair (Marotta et al., 2017). Finally, companies that suffer cyber incidents may face increased premiums and

stricter terms for cybersecurity insurance. Similarly, individuals may find themselves needing to invest more frequently in digital protection tools to stay safe.

Operational Impacts

Operationally, cyber incidents can cause severe disruptions. Attacks like ransomware or Distributed Denial-of-Service (DDoS) can bring core business functions to a halt, delaying important projects, hindering customer interactions, and stalling revenue-generating activities (Eling & Schnell, 2016).

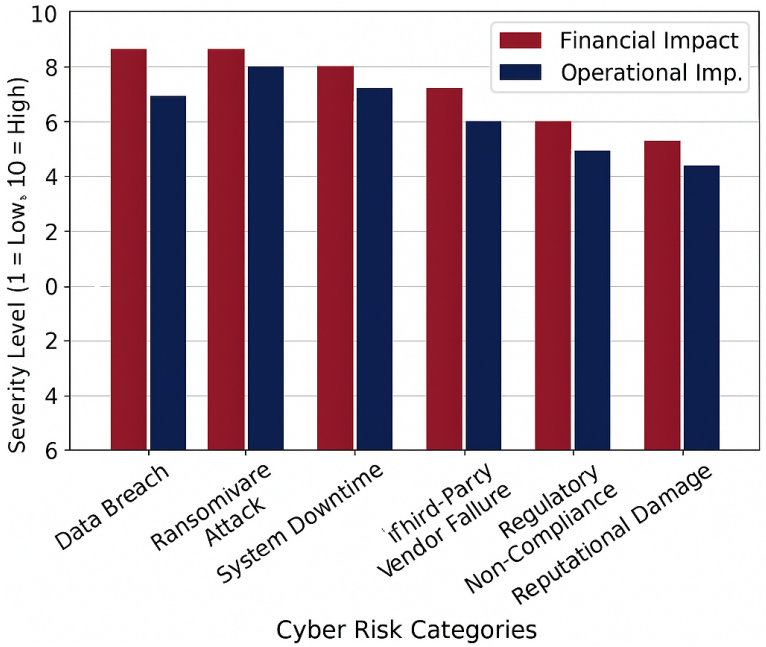
One of the more damaging consequences for businesses is the loss of intellectual property. Hackers often target sensitive data such as research findings, software code, and trade secrets, undermining innovation and competitiveness. Individuals in creative or technical fields can also be affected if their original work is stolen or destroyed.

Cyberattacks also reduce organizational productivity. When employees are locked out of systems or dealing with compromised files, overall efficiency drops, leading to operational slowdowns (OECD, 2021). In more severe cases, critical data may be lost or corrupted entirely, either through unauthorized access or technical failure, with recovery being costly—or sometimes impossible. Individuals may lose important personal files, such as financial records, contracts, or medical documents.

Legal and compliance risks also emerge in the aftermath of cyber incidents. If customer data is compromised, organizations may face lawsuits, investigations, or penalties for failing to meet privacy regulations. While individuals aren't typically held legally responsible, they may still be caught up in legal issues if their stolen identity is used for criminal activity.

Finally, the operational costs of recovering from a cyberattack are often substantial. Companies may need to invest heavily in upgrading IT systems, implementing stronger cybersecurity measures, and providing training for staff. These investments, while necessary, can strain budgets. Likewise, individuals may need to purchase protective software or pay for professional services to enhance their digital security.

Figure (3): Severity of Financial and Operational Impacts of Cyber Risks



The chart highlights the varying severity of financial and operational impacts across six major cyber risks, with Ransomware Attacks and System Downtime ranking highest in financial and operational impact, respectively. These findings align with recent reports, which emphasize the growing cost of ransomware and the critical consequences of service disruption (Kaspersky, 2025; Ponemon Institute, 2022). Regulatory Non-Compliance also scores high financially, reflecting the costly nature of legal penalties under laws like Egypt's Data Protection Law No. 151/2020. Although Reputational Damage scores slightly lower, it remains a significant long-term threat (Biener, Eling, & Wirfs, 2015).

4. Cyber Risk Insurance

4.1. Introduction to Cyber Risk Insurance

In today's hyper-connected global economy, organizations of all sizes rely heavily on digital technologies—cloud computing, digital communications, and remote systems—all of which expose them to a growing spectrum of cyber risks. From data breaches to ransomware attacks, the threat landscape continues to expand in complexity and severity (Marotta et al., 2017). To combat this, cyber risk insurance has become an increasingly important component of business continuity planning and corporate governance.

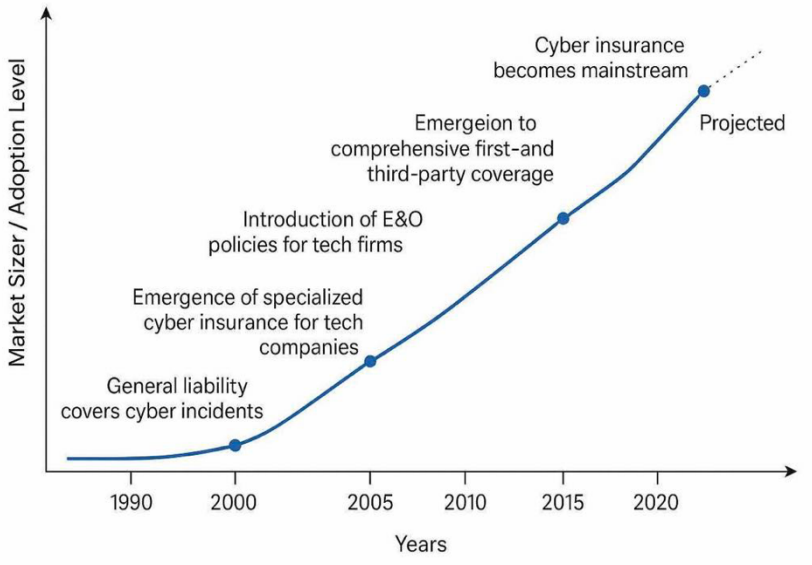
Cyber insurance typically covers two categories of losses: first-party and third-party. First-party coverage includes losses that directly impact the insured, such as data restoration, business interruption, or cyber extortion payments. Third-party coverage handles liabilities, including legal fees, regulatory fines, and claims from customers affected by a breach. As the costs associated with cyber incidents continue to rise, these policies enable businesses to withstand financial shocks, sustain operations, and maintain stakeholder confidence (Romanosky et al., 2019).

4.2. Evolution of Cyber Risk Insurance

Cyber insurance has evolved alongside the growth of digital infrastructure and cyber threats. Initially, before the 1990s, general liability and property policies covered data loss or IT failures, but they were not tailored for cyber-specific risks (Eling & Schnell, 2016). The rise of the internet in the 1990s exposed new vulnerabilities, prompting insurers to offer basic "errors and omissions" (E&O) policies mainly for tech firms to address early-stage data security concerns (Romanosky et al., 2019). In the early 2000s, cyber-specific policies emerged to cover liabilities from data breaches and system failures, spurred by rising awareness and regulatory demands (Biener et al., 2015). Between 2005 and 2015, coverage broadened to include business interruption, ransomware, and legal costs, supported by advancements in actuarial modeling despite limited historical data (Eling & Schnell, 2016). Since 2015, cyber insurance has become central to enterprise risk management, with insurers customizing offerings for sectors like finance, healthcare, and retail, while increasingly targeting SMEs (OECD, 2017).

Regulations like the GDPR and Canada's PIPEDA have increased demand for insurance coverage by mandating breach reporting and data protection (OECD, 2021). Despite rapid adoption, the market still faces challenges, including a lack of actuarial data, constantly evolving threats, and aggregation risks from large-scale attacks (Biener et al., 2015; Eling & Schnell, 2016). To address these issues, insurers are turning to artificial intelligence and machine learning for better risk modeling and policy customization (Marotta et al., 2017). Regulators are recognizing the strategic value of cyber insurance in economic resilience. In emerging markets such as Egypt, where digital transformation is accelerating, cyber insurance has strong potential to help businesses manage growing cyber threats (OECD, 2021).

Figure (4): Evolution of the Cyber Insurance Market (1990–2025)



This graph illustrates the progressive growth and maturity of the cyber insurance industry over time. It shows a slow start in the 1990s when cyber risks were minimally addressed under general liability policies, followed by a steady increase after the introduction of E&O policies and specialized cyber coverage in the early 2000s. The sharp upward trend after 2015 reflects the growing recognition of cyber

risk as a mainstream business threat, driven by regulatory changes and high-profile cyberattacks. The projected growth beyond 2025 highlights industry expectations for continued expansion, especially in emerging markets.

The following table provides a comparative overview of cyber insurance premium growth across selected countries, highlighting both current market maturity and projected expansion potential through 2025.

Table (2): Growth of Cyber Insurance Premiums (2020–2025) and Market Share in Selected Countries

Country	2020 Cyber Premiums	2023 Cyber Premiums	2025 (Projected)	% of Total Premiums (2023)
Canada	$750M CAD	$1.8B CAD	$2.5B CAD	3.5%
South Africa	$45M USD	$85M USD	$140M USD	1.2%
Saudi Arabia	$120M USD	$320M USD	$600M USD	2.8%

Sources: Swiss Re – Cyber Insurance Market Reports, A.M. Best – Global Cyber Insurance Outlook, Insurance Regulatory Authorities in each country, PwC – Global Cyber Insurance Survey, McKinsey & Co. – Cyber Risk and Insurance Trends

Table (2) shows that Canada has the most mature cyber insurance market among the listed countries, with premiums growing from $750 million CAD in 2020 to $1.8 billion CAD in 2023, and projected to reach CAD 2.5 billion by 2025. Cyber insurance accounts for 3.5% of Canada's total insurance premiums, reflecting strong awareness, regulatory requirements, and digital infrastructure.

South Africa shows more moderate growth, with cyber premiums rising from $45 million USD in 2020 to $85 million USD in 2023 and expected to reach $140 million USD by 2025. However, cyber insurance represents just 1.2% of the country's total premiums, indicating potential for further development in the market.

Saudi Arabia demonstrates rapid expansion in its cyber insurance sector, growing from $120 million USD in 2020 to $320 million USD in 2023, with a projection of $600 million USD by 2025. Cyber premiums make up 2.8% of total insurance premiums, suggesting strong investment in cybersecurity and increased demand for risk transfer solutions in a digitally advancing economy.

4.3.Core Components and Importance of Cyber Risk Insurance

Cyber insurance is built around two primary components: first-party and third-party coverage. First-party coverage addresses direct losses an organization suffers after a cyberattack, such as data restoration, business interruption, ransom payments, forensic investigations, and breach notifications (Woods &

Simpson, 2017). Third-party liability coverage protects against external claims from customers, partners, or regulators, covering legal defence costs, regulatory fines (under laws like GDPR and PIPEDA), and compensation for affected individuals (OECD, 2017). As cyber threats grow more frequent and complex, cyber insurance has become essential for modern businesses by providing financial protection that enables faster recovery and minimal disruption (Woods & Simpson, 2017). According to IBM's 2024 report, the global average cost of a data breach has reached $4.45 million, highlighting the urgency of adequate coverage (IBM, 2024). Small and medium-sized enterprises (SMEs) are particularly vulnerable due to limited security resources, while global privacy laws demand timely breach notification and penalize non-compliance. In this context, cyber insurance not only offsets financial losses but also enhances regulatory compliance, crisis management, and overall risk transfer strategies (Böhme & Schwartz, 2010; OECD, 2017).

5. Cyber Risk Insurance in Egypt

5.1. Overview of the Egyptian Insurance Market

As Egypt rapidly embraces digital transformation, the risks posed by cyber threats are becoming more severe and frequent, affecting both businesses and government institutions. This shift underscores the growing need for cyber risk insurance to protect against financial and operational consequences. Although the Egyptian cyber insurance market is still in its early stages, it is gradually developing due to increasing digital adoption, heightened awareness, and regulatory progress—especially the introduction of Data Protection Law No. 151 of 2020. However, the law's enforcement remains weak, and many businesses lack awareness of available cyber insurance options, pointing to the need for stronger regulation, education, and stakeholder coordination (Tawfik, 2022).

Egypt's insurance sector, one of the oldest in the MENA region, is regulated by the Financial Regulatory Authority (FRA), which oversees both life and non-life segments. While life insurance focuses on death, disability, and income replacement, non-life insurance includes property, auto, health, and recently, cyber risk coverage (FRA, 2022). Despite overall market growth, cyber insurance is still a niche product with limited penetration. Only a few insurers currently offer cyber-specific policies, which typically cover data breaches, business interruptions, ransomware, third-party liabilities, and incident response. These products are generally targeted at larger enterprises with strong digital infrastructure, leaving SMEs underserved and highlighting the market's need for more accessible and standardized solutions.

5.2. Challenges and Future Prospects for Cyber Risk Insurance in Egypt

The development of cyber insurance in Egypt faces several key challenges. One major issue is the low awareness of cyber risks, especially among SMEs, which often underestimate the potential financial and reputational damage from cyberattacks (OECD, 2021). Many businesses also rely on outdated cybersecurity systems, increasing underwriting risks and discouraging insurer participation.

Another significant barrier is the lack of historical data, making it difficult for insurers to accurately price cyber risk. Without reliable incident and loss reporting, actuarial modelling remains limited (Biener et

al., 2015). Regulatory gaps, including unclear breach reporting obligations and liability rules, further complicate the development of effective policies.

The high cost of cyber insurance also deters adoption, particularly among smaller businesses that may not see the immediate value. Additionally, the threat of aggregation risk—where a single cyber event impacts multiple policyholders—adds to insurer caution. Low insurance penetration, limited local cyber underwriting expertise, and slow digital adoption continue to hinder market growth (Eling & Schnell, 2016; OECD, 2021).

Despite these challenges, Egypt's cyber insurance market holds strong growth potential. Increasing digitalization, more frequent cyber threats, and stronger regulatory backing are laying the groundwork for expansion. High-risk sectors like finance, telecommunications, and healthcare are expected to lead the demand for cyber coverage (ENISA, 2023; FRA, 2022).

Government initiatives such as the Personal Data Protection Law and a national cybersecurity strategy reflect a growing commitment to data protection. These policies are likely to drive compliance needs and encourage more businesses to adopt cyber insurance as a financial safety net (OECD, 2022; Egyptian Ministry of Communications and Information Technology, 2021).

Improving awareness remains essential, especially among SMEs. Educational campaigns from insurers and public agencies can help close the knowledge gap and highlight the value of cyber insurance (Swiss Re Institute, 2023; World Bank, 2022). As the market matures, insurers are also expected to offer more tailored products.

Future offerings may include flexible policies suited to different business sizes and sectors. Bundling insurance with services like security assessments, employee training, and breach response can add further value and improve adoption (Accenture, 2024; Allianz, 2023).

6. Cyber Risk Insurance Pricing: Key Factors and Advanced Methodologies

Setting prices for cyber risk insurance is one of the most complex tasks in today's insurance industry. Unlike traditional insurance lines such as property or auto, cyber risk is constantly evolving, difficult to quantify, and often lacks the historical data needed for accurate pricing. This makes it challenging for insurers to develop consistent pricing models (Biener et al., 2015; Eling & Schnell, 2016).

6.1. Main Factors Affecting Cyber Risk Insurance Pricing

Several elements influence how insurers determine premiums for cyber insurance policies. A primary factor is the insured organization's level of exposure to cyber threats. Larger companies or those in high-risk sectors like finance, healthcare, or technology—where sensitive data is routinely handled—tend to face higher premiums. These businesses are more attractive targets for cybercriminals and could face greater financial losses in the event of a breach (Romanosky et al., 2019; OECD, 2017).

The strength of an organization's cybersecurity practices is also important. Companies that implement strong security measures—like encryption, two-factor authentication, and regular security audits—are

seen as lower risk and may qualify for discounts. On the other hand, a history of frequent or severe claims typically leads to higher premiums (Woods & Simpson, 2017; Biener et al., 2015).

Coverage type and policy limits also play a role. Broader policies that include protection for ransomware attacks, business interruption, and regulatory penalties tend to cost more due to the greater financial exposure for insurers. Similarly, higher coverage limits or lower deductibles increase the potential payout, raising the premium (OECD, 2018).

Regulatory environments affect pricing as well. Companies operating in regions with strict data protection laws—such as GDPR in Europe or CCPA in California—may pay more due to the high penalties for non-compliance. Organizations in high-risk geographic areas or those with weak cyber enforcement may also face elevated costs (Talesh, 2018; Marotta et al., 2017).

Finally, insurers consider an organization's public profile. Companies with strong brand reputations or high media visibility could suffer significant reputational damage from a cyberattack. Insurers factor this into premium pricing, accounting for potential crisis management and customer trust recovery costs (Romanosky et al., 2019).

In short, cyber insurance pricing depends on a combination of internal risk factors, external threats, regulatory context, and historical claims data. Insurers must continuously adapt their models to keep up with the shifting nature of cyber risks.

6.2. Methodologies and Techniques for Quantifying and Pricing Cyber Risk Insurance

Quantifying and pricing cyber risk is a complex and evolving process, shaped by the unique nature of cyber threats—marked by uncertainty, lack of historical data, and dynamic threat landscapes. Insurers rely on a range of tools, techniques, and pricing methodologies to assess risk exposure and determine appropriate premiums for cyber insurance policies.

6.2.1. Quantitative Risk Assessment Models

To evaluate potential losses from cyber incidents, insurers employ quantitative risk assessment tools traditionally used in finance and engineering:

- Value-at-Risk (VaR): This technique estimates the maximum expected loss from a cyber event over a specified period under normal conditions. It provides a probabilistic measure of loss severity, helping insurers assess capital reserves (Eling & Schnell, 2016).
- Monte Carlo Simulations: By simulating thousands of cyber event scenarios based on defined probability distributions, Monte Carlo models help estimate potential losses and understand the range of possible outcomes. This is particularly useful for modelling low-frequency, high-impact events (Radanliev et al., 2020).
- Scenario Analysis and Stress Testing: Insurers simulate cyber incidents such as ransomware attacks or data breaches to evaluate financial impact under extreme or worst-case conditions. This helps in understanding exposure and pricing insurance products accordingly (Romanosky et al., 2019; Eling & Schnell, 2016).

6.2.2. Cyber Risk Rating Systems

- Third-Party Cyber Risk Ratings: Agencies like BitSight, Security Scorecard, and Up Guard provide cybersecurity health scores based on external scans and public data (e.g., patching cadence, exposed ports, malware presence). Insurers integrate these ratings to assess the risk exposure of potential clients (Marotta et al., 2017).
- Internal Risk Scores: Based on a company's cybersecurity posture—including security policies, incident response plans, and employee training—insurers assign scores that influence premium pricing. Lower scores (stronger security) typically correspond to reduced premiums (Woods & Simpson, 2017).

6.2.3. Use of Historical Data and Loss Distribution Models

- Claims Data Analysis: Insurers analyze past cyber insurance claims to identify patterns in frequency and severity. This data, though still emerging, helps calibrate pricing models and inform underwriting decisions (Biener et al., 2015).
- Loss Distribution Models: These models estimate the probability and magnitude of losses. They are particularly useful in quantifying tail risks—rare but severe events—that are characteristic of cyber exposures (Eling & Schnell, 2016).

6.2.4. Market Benchmarking

- Cyber Insurance Market Benchmarks: Comparing pricing strategies and loss experiences across sectors and regions helps insurers align their offerings with market standards, ensuring competitiveness and sustainability (OECD, 2018).

6.2.5. Innovative Pricing Methodologies

Given the scarcity of long-term historical data, traditional actuarial models are supplemented by more dynamic approaches:

- Actuarial Models: While foundational, actuarial methods are limited due to cyber risk's volatility and novelty. Actuaries increasingly rely on expert judgment, industry proxies, and Bayesian inference (Biener et al., 2015; Eling & Schnell, 2016).
- Risk-Based Pricing Models: These models tie premium rates to an organization's cybersecurity defences and risk management practices. Organizations with robust controls receive preferential pricing, incentivizing improved cyber hygiene (Woods & Simpson, 2017).
- Event-Driven Pricing Models: Insurers assess the likelihood of specific threat vectors (e.g., phishing, malware, DDoS) and adjust premiums based on threat exposure and incident trends across similar firms or sectors (Romanosky et al., 2019).

6.2.6. Use of Advanced Analytics and Machine Learning

- Predictive Analytics and Machine Learning: The application of AI techniques enables insurers to analyze large, multidimensional datasets—including threat intelligence feeds, behavioural data, and real-time cyber events. These tools enhance risk prediction, identify emerging threats, and support granular pricing models (Boehme & Kataria, 2020; Woods & Moore, 2020).

- Collaboration with Cybersecurity Providers: Partnerships between insurers and cybersecurity firms facilitate real-time monitoring and assessments, providing insurers with better visibility into insureds' security postures and enabling dynamic risk-based pricing (Radanliev et al., 2020).

7. Cyber Insurance Pricing Model Using Monte Carlo Simulation for the Egyptian Market

To address the increasing complexity and unpredictability of cyber risks in emerging markets like Egypt, this study presents two advanced simulation models designed to support data-driven pricing decisions in cyber insurance.

The first is a Probabilistic Pricing Model, which uses scenario-based Monte Carlo simulations to estimate average claim costs and set appropriate premiums. It accounts for different levels of cyber threat exposure, operational risk, and the maturity of the local insurance market, offering a realistic reflection of underwriting conditions.

The second is an Annual Cyber Loss Simulation Model, which estimates the frequency and impact of cyber incidents using Poisson and normal distribution methods. This model helps evaluate the profitability of underwriting by calculating expected returns, volatility, the likelihood of losses, and the long-term net present value (NPV) across various types of businesses.

Together, these models equip insurers with practical and analytical tools to improve pricing accuracy, better manage risk portfolios, and build more sustainable cyber insurance strategies.

7.1. Pricing Model Based on Probabilistic Risk Modelling Approach

This Monte Carlo simulation is based on a probabilistic risk modelling approach designed to support cyber insurance pricing decisions. Specifically, it simulates potential claim cost outcomes under different market conditions to help insurers set appropriate premiums. Model Foundations:

1. Risk Assumptions per Scenario: Optimistic, Moderate, and Pessimistic scenarios represent different levels of cyber threat severity and operational exposure, modelled to reflect real-world uncertainty in the Egyptian insurance market.
    - **Optimistic Scenario**: Assumes lower average claim costs (EGP 50,000) with limited variability (std dev EGP 10,000).
    - **Moderate Scenario**: Assumes moderate claim costs (EGP 100,000) and variability (std dev EGP 20,000).
    - **Pessimistic Scenario**: Assumes high costs (EGP 200,000) and higher uncertainty (std dev EGP 30,000).
2. Normal Distribution: Claim cost outcomes are modelled using a normal (Gaussian) distribution, defined by a mean (expected cost) and standard deviation (variability). This assumes most claims are around the mean, with fewer extreme outcomes.
3. 10,000 Iterations: The Monte Carlo technique runs 10,000 simulations per scenario, generating a distribution of possible outcomes. This allows the insurer to see not just the average cost but the full range of potential claims.

4. Premium Calculation Rule: Premiums are calculated using a pricing multiplier applied to the average simulated claim cost: Optimistic: 1.3x, Moderate: 1.5x, Pessimistic: 1.7x. These multipliers reflect risk appetite, administrative overheads, profit margin, and capital reserve needs.

This Monte Carlo simulation uses a probabilistic risk modelling approach to support cyber insurance pricing decisions by estimating potential claim costs under varying market conditions. It helps insurers determine appropriate premiums by accounting for different levels of risk and uncertainty. Key Model Components:

1. Risk Assumptions per Scenario: The model includes three scenarios—Optimistic, Moderate, and Pessimistic—each reflecting different degrees of cyber threat severity and operational exposure, tailored to the context of Egypt's insurance market.

    - In the Optimistic scenario, average claim costs are set at EGP 50,000 with low variability (standard deviation of EGP 10,000).
    - The Moderate scenario assumes claim costs of EGP 100,000 with a standard deviation of EGP 20,000.
    - The Pessimistic scenario projects higher claim costs at EGP 200,000 and greater uncertainty (standard deviation of EGP 30,000).

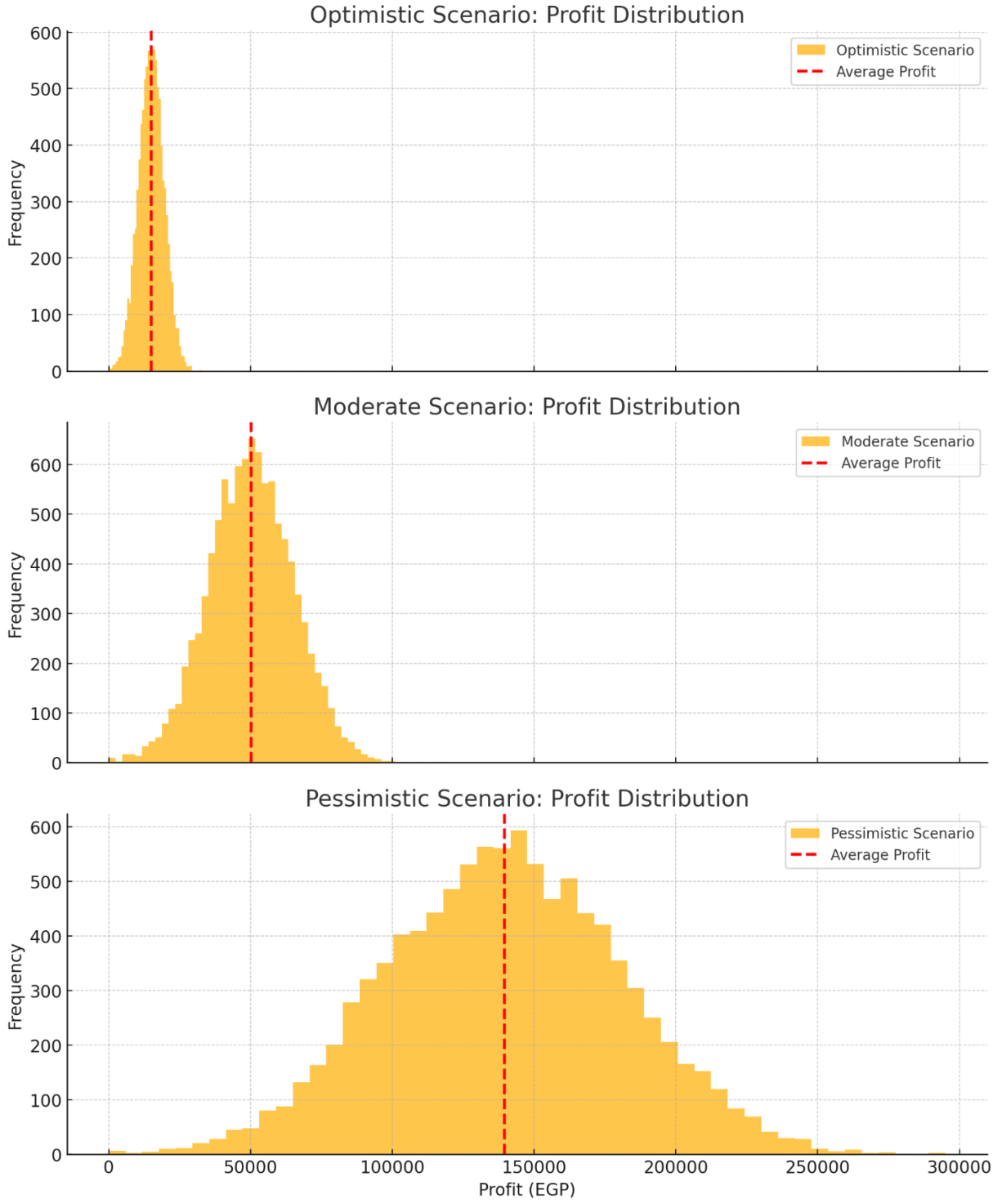
2. Normal Distribution Modelling: Claim costs are modelled using a normal (Gaussian) distribution, with outcomes centred around the average and a smaller probability of extreme values.

3. Simulation Runs: Each scenario is simulated 10,000 times to generate a wide range of potential outcomes. This provides a comprehensive view of possible claim distributions beyond just average values.

4. Premium Calculation Rule: Premiums are calculated by applying a specific multiplier to the average simulated claim cost to account for risk, operational costs, profit margins, and reserves: Optimistic: 1.3x average cost, Moderate: 1.5x, Pessimistic: 1.7x.

This structured approach allows insurers to price cyber insurance products more accurately while factoring in market uncertainty and risk exposure.

Figure (5): Distribution of Profits Under Different Cyber Insurance Scenarios



7.1.1. Summary of Simulation Results

Table (3): Summary of Simulation Results for Claim Costs, Premiums, and Profitability Across Different Scenarios

Scenario	Mean Claim Cost	Mean Premium per Policy	Average Profit per Policy	Probability of Loss
Optimistic	EGP 50,000	EGP 65,000	EGP 14,991	0.0%
Moderate	EGP 100,000	EGP 150,000	EGP 50,204	0.0%
Pessimistic	EGP 200.000	EGP 340,000	EGP 139,479	0.0%

7.1.2. Discussion of Simulation Results

The Monte Carlo simulation provided insights into the financial performance of cyber risk insurance under three scenarios tailored to the Egyptian market. Each scenario reflected varying levels of cyber threat frequency, claim severity, and pricing strategies. Here is a comparative analysis:

7.1.2.1. Optimistic Scenario

- Incident Rate: 5%
- Mean Claim Cost: EGP 50,000
- Standard Deviation: EGP 10,000
- Premium Charged: EGP 65,000 (1.3 × EGP 50,000)
- Average Profit per Policy: EGP 14,991
- Profit Margin: 23%
- Loss Probability: 0.0% (based on 10,000 Monte Carlo simulations)

In this scenario, which reflects digitally mature and well-protected firms in urban Egypt, the model assumes a low incident frequency of 5% and moderate claim severity. The relatively low premiums of EGP 65,000 were sufficient to generate a consistent average profit of EGP 14,991 per policy, with no losses observed across all simulation trials. This confirms that even with moderate pricing, insurers can remain profitable in low-risk environments.

Such market segments—likely comprising large, cyber-aware companies with strong internal controls—offer promising opportunities for insurers. Targeting these clients with affordable and stable insurance products can increase adoption while maintaining financial sustainability. The findings also encourage risk-based segmentation and pricing strategies, particularly for emerging markets like Egypt, where cyber readiness varies widely.

7.1.2.2. Moderate Scenario

- Incident Rate: 10%
- Mean Claim Cost: EGP 100,000
- Standard Deviation: EGP 20,000
- Premium Charged: EGP 150,000 (1.5 × EGP 100,000)
- Average Profit per Policy: EGP 50,204
- Profit Margin: 33%
- Loss Probability: 0.0% (based on 10,000 Monte Carlo simulations)

This scenario represents typical Egyptian small and medium-sized enterprises (SMEs) that are currently undergoing digital transformation but are not yet fully secured. With a claim frequency assumed to be moderate and premiums set at EGP 150,000, the insurer earns a solid profit margin of 33%. The Monte Carlo simulation showed no probability of loss, suggesting that this pricing approach provides sufficient risk coverage while remaining accessible to businesses.

Given its balance between affordability and profitability, this model is likely the most realistic for broad market adoption in Egypt. It offers a benchmark for insurers seeking to develop scalable cyber insurance products that can serve the growing digital economy without exposing themselves to excessive financial risk.

7.1.2.3. Pessimistic Scenario

- Incident Rate: 20%
- Mean Claim Cost: EGP 200,000
- Standard Deviation: EGP 30,000
- Premium Charged: EGP 340,000 (1.7 × EGP 200,000)
- Average Profit per Policy: EGP 139,479
- Profit Margin: 41%
- Loss Probability: 0.0% (based on 10,000 Monte Carlo simulations)

This scenario reflects the realities of Egypt's most vulnerable digital businesses—particularly those operating in rural areas or under weak regulatory oversight, with limited cybersecurity infrastructure. It assumes a high frequency and severity of claims, leading to a significantly higher premium of EGP 340,000 per policy.

Despite the elevated risks, the model remains highly profitable, with an average profit of EGP 139,479 per policy and no recorded losses in the simulation. This underscores the effectiveness of a robust risk-loading strategy. However, the high premium required to ensure sustainability may deter SMEs from participating, making affordability a key concern. Policymakers and insurers may need to explore subsidies, phased premiums, or public-private partnerships to encourage uptake in this high-risk group.

7.2. Pricing Model Based on Annual Cyber Losses

This Monte Carlo simulation models annual cyber losses for five types of organizations, assessing both profitability and underwriting risk, and provides insurers with data-driven guidance for pricing cyber insurance across various business risk profiles. Model Foundations:

1. Organizational Risk Segments: The simulation considers five distinct profiles:

- Low Risk Organization
- Moderate Risk Organization
- High Risk Organization
- Tech Firm (High Severity)
- Retail Chain (High Frequency)

Each group reflects unique characteristics in terms of attack frequency and loss severity.

2. Statistical Distributions:

- Cyber Attack Frequency: Modelled with a Poisson distribution, ideal for counting random events (i.e., to simulate the number of attacks per year).
- Loss Severity per Attack: Modelled using a normal distribution, capturing average and variability in loss amounts (to model the severity of each incident) with: [Mean = average loss per attack, Std. Dev. = 30% of the average loss (to simulate real-life volatility), and Losses were clipped to prevent negative values].

3. Financial Metrics: For each scenario, the model calculates:

- Average Annual Loss: Total simulated losses per year = sum of all attack losses for that year.
- Standard Deviation (Volatility)
- Expected Annual Profit: $\text{Profit}_{\text{year}}$ = Premium−Total Annual Loss
- Loss Probability (%) – likelihood that underwriting leads to a net loss each year
- Net Present Value (NPV) over 5 Years: applying a 5% discount rate to reflect the time value of money: NPV = $\sum_{t=1}^{5} \frac{\text{Profit}_t}{(1+0.05)^t}$

4. Premium Assumptions: Each organization type is assigned a predefined premium based on current market expectations. This allows for a realistic simulation of underwriting performance without overestimating profitability.
5. Simulation Scale: Each profile undergoes 10,000 simulation runs to produce a robust set of outcomes, enabling insurers to understand not just average results, but also the distribution of possible scenarios—critical for managing pricing and risk effectively.

Table (4): Cyber Risk Scenarios and Proposed Premiums for the Egyptian Insurance Market

Scenario Name	Mean Attacks/Year	Average Loss/Attack (EGP)	Proposed Premium (EGP)
Low Risk Org	0.5	30,000	19,586.86
Moderate Risk Org	1.5	50,000	97,425.93
High Risk Org	3.0	70,000	239,049.83
Tech Firm (High Severity)	1.0	150,000	122,725.42
Retail Chain (High Freq.)	5.0	25,000	162,524.17

Figure (6): Monte Carlo Simulation Results for Cyber Insurance Scenarios

7.2.1. Summary of Simulation Results

Table (5): Summary of Simulation Results – Annual Losses, Standard Deviation, NPV, Profitability, and Loss Probability by Organization Type

Scenario	Avg Annual Loss (EGP)	Std Dev (EGP)	NPV (5 Yr)	Loss Prob (NPV)	Expected Profit (EGP)	Loss Probability (%)
Low Risk Org.	15,146.06	22,250	~21,000	~32%	4,440	35.85%
Moderate Risk Org.	75,274.71	64,837	~97,000	~29%	22,151	32.75%
High Risk Org.	209,471.68	124,797	~132,000	~35%	29,578	36.59%
Tech Firm (High Severity)	151,662.22	157,744	**–29,000**	**>50%**	**-28,936**	**53.85%**
Retail Chain (High Freq.)	125,865.27	58,343	~165,000	~22%	36,658	25.51%

7.2.2. Discussion of Simulation Results

The simulation revealed important insights into the financial behaviour of cyber risk insurance across various types of organizations, highlighting how differences in attack frequency and loss severity affect profitability.

Retail Chains emerged as one of the more stable and profitable segments. Although they experience frequent cyberattacks, the resulting losses tend to be relatively minor. This combination of high frequency and low severity makes them a favourable target for insurers, offering both predictability and financial returns.

Tech Firms, on the other hand, presented a much riskier picture. These organizations showed high variability in loss outcomes and suffered from severe incidents. As a result, they generated average underwriting losses and carried a 53.85% likelihood of ending the year in a deficit. This suggests that current pricing models may underestimate the true level of risk, pointing to a need for premium adjustments or stricter underwriting.

Low and Moderate Risk Organizations produced modest profits but with a considerable risk of loss, ranging from 30% to 36%. These figures imply that while they may appear attractive, their profitability

is not guaranteed unless insurers can offset the risk through bundling policies or operating at a larger scale.

Lastly, High Risk Organizations displayed strong profit potential but came with substantial unpredictability. The wide variation in outcomes suggests that these clients represent a high-risk, high-reward opportunity. Insurers interested in this segment would likely need to consider protective measures such as reinsurance to manage volatility.

Overall, the simulation underscores the importance of tailoring cyber insurance strategies based on organizational risk profiles, helping insurers balance profitability with long-term sustainability.

8. Hypothesis Results

H1: A simulation-based pricing model will yield premiums that align more closely with the actual risk exposure compared to traditional fixed-rate pricing methods.
The simulation results supported this hypothesis by producing significantly different expected annual losses for each type of organization, which in turn allowed for tailored premium recommendations. For instance, the Low-Risk Organization showed an expected annual loss of around 15,146 EGP, supporting a premium of 19,586 EGP. In contrast, the High-Risk Organization had annual losses exceeding 209,000 EGP, justifying a much higher premium. These distinctions clearly show that simulation-based pricing offers a more accurate and risk-sensitive approach than the one-size-fits-all strategy of traditional pricing models.

H2: The incorporation of deductibles and NPV analysis over multi-year periods will enhance the model's ability to project profitability and manage long-term underwriting risk.
By analyzing Net Present Value (NPV) over five years, the model offered a more strategic, forward-looking assessment of profitability. For example, while the Tech Firm scenario showed a positive annual profit, its long-term NPV was negative due to the high volatility of losses, highlighting long-term risk. When deductibles were introduced, they helped reduce exposure to smaller, frequent claims, improving both NPV and reducing loss probabilities in cases like the Retail Chain. This demonstrates that incorporating deductibles and multi-year projections strengthens pricing strategies and helps manage long-term underwriting risk more effectively.

9. Recommendations

The dual-model Monte Carlo simulation framework offers a robust, data-driven approach to setting cyber insurance premiums in Egypt. These two models complement each other by providing different insights into risk exposure, claim volatility, and pricing strategies. Based on the findings from both the Probabilistic Risk Modelling Approach and the Annual Cyber Loss Simulation, several recommendations emerge:

1. Adopt Tiered Pricing with Risk-Based Multipliers: The probabilistic model suggests using scenario-specific multipliers to set premiums according to varying levels of risk, overhead, and capital requirements: Optimistic (low uncertainty) 1.3× multiplier, Moderate (medium

uncertainty) 1.5× multiplier, Pessimistic (high uncertainty) 1.7× multiplier. This structured approach allows insurers to price different risk levels systematically while maintaining profitability, with all scenarios showing no loss probability.

2. Segment Risk by Frequency and Severity: The Annual Cyber Loss Model highlights the importance of categorizing clients based on how often they experience attacks and the severity of losses, enabling more accurate risk assessment.
3. Include Deductible Modelling: Introducing deductibles in the simulation significantly lowers expected losses, particularly for portfolios with frequent claims. Deductibles serve as a first line of defence against small claims and are a common cost-control measure in cyber insurance.
4. Use Net Present Value (NPV) for Long-Term Planning: The framework includes a 5-year NPV analysis at a 5% discount rate, aligning pricing with long-term profitability goals. Some scenarios, like tech firms, show high long-term financial risk despite short-term profits, signalling that insurers should avoid underpricing based on short-term gains alone.
5. Incorporate Confidence Intervals: Adding confidence intervals (e.g., 95%) to profit and NPV estimates enhances risk understanding. This allows underwriters and actuaries to prepare for worst-case outcomes and build resilience into pricing. For example, a tech firm's 95% confidence interval might reveal potential five-year losses exceeding EGP 100,000.
6. Customize Products by Risk Profile: Using scenario outputs, insurers can tailor policies to different risk levels:
    - Low-risk organizations: Standard coverage with low premiums and deductibles
    - Moderate-risk organizations: Moderate premiums with optional add-ons such as breach response or legal coverage
    - High-risk and tech firms: Premium plans featuring higher deductibles, loss limits, and shared risk options
7. Significance for Egypt's Cyber Insurance Market: These simulations provide critical support for Egypt's emerging cyber insurance sector by:
    - Offering a scientific pricing method despite limited data
    - Serving as a benchmark for assessing portfolio health
    - Encouraging product innovation based on client risk profiles
    - Providing a framework to engage regulators, helping justify premiums to both clients and authorities

10. References

Abbast, M. (2025). Insights from Kaspersky META 2025 Middle East Cyber Threat Analysis Report: Ransomware, SideWinder, and more. Medium. https://mahdiabbastech.medium.com/insights-from-kaspersky-meta-2025-middle-east-cyber-threat-analysis-report-ransomware-sidewinder-682a9f8ee066

Abdelmottaleb, M., & Soliman, M. (2020). Insurance innovation in Egypt: Challenges and opportunities. Middle East Insurance Review, 34(6), 18–22.

Accenture. (2024). Cyber Insurance and AI-Driven Risk Modelling. Accenture Reports.

Allianz. (2023). Cyber Risk Barometer: Emerging Risks in MENA. Allianz Global Corporate & Specialty.

Antonio, Y., Indratno, S. W., & Saputro, S. W. (2021). Pricing of cyber insurance premiums using a Markov-based dynamic model with clustering structure. PLOS ONE, 16(10), e0258867. https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0258867

Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A., & Weber, S. (2023). Modelling and pricing cyber insurance: Idiosyncratic, systematic, and systemic risks. European Actuarial Journal, 13(1), 1–53. https://link.springer.com/article/10.1007/s13385-023-00341-9

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. The Geneva Papers on Risk and Insurance, 40(1), 131–158.

Böhme, R. (2005). Cyber-Insurance Revisited. In Proceedings of the Workshop on the Economics of Information Security(WEIS), Kennedy School of Government, Cambridge, MA. Technische Universität Dresden, Institute for System Architecture.

Böhme, R., & Kataria, G. (2020). Models and Measures for Correlation in Cyber-Insurance. In R. Böhme & T. Moore (Eds.), The Economics of Information Security and Privacy (pp. 143–166). Springer.

Böhme, R., & Schwartz, G. (2010). Modelling cyber-insurance: Towards a unifying framework. WEIS.

Egyptian Financial Regulatory Authority (FRA). (2022). Annual Report on the Insurance Sector.

Egyptian Financial Regulatory Authority (FRA). (2022). Annual Report on Insurance Sector Development in Egypt.

Egyptian Ministry of Communications and Information Technology. (2021). National Cybersecurity Strategy.

Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? Journal of Risk Finance, 17(5), 474–491.

ENISA. (2023). Threat Landscape Report 2023. European Union Agency for Cybersecurity.

Herzog, T. N. (2011). Introduction to Monte Carlo methods. In T. N. Herzog, Data Quality and Record Linkage Techniques (pp. 245–260). Springer.

Hua, L., & Xu, M. (2020, June 29). Pricing cyber insurance for a large-scale network (arXiv:2007.00454) [Preprint]. arXiv. https://arxiv.org/abs/2007.00454

IBM. (2024). Cost of a Data Breach Report 2024. https://www.ibm.com/security/data-breach

Ioannidis & Skeoch, H. R. K., C. (2024). The barriers to sustainable risk transfer in the cyber-insurance market. Journal of Cybersecurity, 10(1), Article tyae003. https://academic.oup.com/cybersecurity/article/10/1/tyae003/7610985

Maillart, T., & Sornette, D. (2010). Heavy-tailed distribution of cyber-risks. The European Physical Journal B, 75(3), 357–364.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., & Yautsiukhin, A. (2017). Cyber-insurance survey. Computer Science Review, 24, 35–61.

OECD (2017), Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris, https://www.oecd.org/en/ Understanding the Insurance Protection Gap for Cyber Risk publications/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en.html

OECD. (2018). https://www.oecd.org/finance/insurance

OECD. (2021). Strengthening Cybersecurity Governance in Egypt. Retrieved from https://www.oecd.org

OECD. (2022). Cyber Insurance in Emerging Economies: Trends and Barriers. Organization for Economic Co-operation and Development.

OECD. (2022a). Enhancing the Role of Insurance in Managing Cyber Risk. OECD Publishing.

Office of the Privacy Commissioner of Canada. (2022). PIPEDA breach reporting.

PwC. (2022). Cyber insurance: Risk and resilience in the digital age. Retrieved from https://www.pwc.com

Radanliev, P., De Roure, D., Nurse, J. R. C., & Montalvo, R. M. (2020). Artificial intelligence and machine learning in dynamic cyber risk analytics at the edge. Computers in Industry, 124, 103387.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? Journal of Cybersecurity, 5(1).

Skeoch, H. R. K., & Pym, D. J. (2023). Pricing cyber-insurance for systems via maturity models (arXiv:2302.04734) [Preprint]. arXiv. https://arxiv.org/abs/2302.04734

Swiss Re Institute. (2023). Global Insurance Review: Focus on Cyber Risk in the MENA Region.

Talesh, S. A. (2018). Data breach, privacy, and cyber insurance: How insurance companies act as "compliance managers" for businesses. Law & Social Inquiry, 43(2), 417–440.

Tawfik, N. (2022). Data Protection Law in Egypt: Challenges and Opportunities. Middle East Law and Governance, 14(2), 220–243.

Woods, D., & Moore, T. (2020). Does insurance have a future in governing cybersecurity? IEEE Security & Privacy, 18(1), 21–27.

Woods, D., & Simpson, A. (2017). Policy measures and cyber insurance: A framework. Journal of Cyber Policy, 2(2), 209–226.

World Bank. (2022). Improving Cyber Resilience in Developing Economies.

11.Codes for Simulation

- **Python code for Figure (1): Impact of Key Challenges on Cyber Insurance Pricing in Egypt**

```python
import matplotlib.pyplot as plt

# Define challenges and their impact levels (on a scale of 1–10)
challenges = [
    "Lack of Historical Data",
    "Evolving Cyber Threats",
    "Digital Infrastructure Dependency",
    "Absence of Local Models",
    "Weak Threat Intelligence Integration"
]
impact_on_pricing = [9, 8, 7, 8, 7]

# Create the bar chart
plt.figure(figsize=(10, 6))
bars = plt.barh(challenges, impact_on_pricing, color='royalblue')
plt.xlabel("Impact Level on Pricing Accuracy (1 = Low, 10 = High)")
plt.title("Impact of Key Challenges on Cyber Insurance Pricing in Egypt")
plt.xlim(0, 10)

# Add labels to bars
for bar in bars:
    width = bar.get_width()
    plt.text(width + 0.1, bar.get_y() + bar.get_height()/2,
             f"{width}", va='center')

plt.gca().invert_yaxis()  # Highest impact at top
plt.tight_layout()
plt.show()
```

- **Python code for Figure (2): Estimated Distribution of Cyber Risk Types (Global Approximation)**

```python
import matplotlib.pyplot as plt

# Define categories of cyber risks
categories = [
    "Cybersecurity Threats",
    "Operational Risks",
    "Financial Risks",
    "Legal & Compliance Risks",
    "Reputational Risks",
    "Strategic Risks",
    "Privacy Risks"
]

# Estimated % of cyber incidents involving each risk category
percentages = [35, 15, 12, 10, 8, 10, 10]

# Create pie chart
plt.figure(figsize=(8, 8))
colors = plt.cm.tab20c.colors
plt.pie(percentages, labels=categories, autopct='%1.1f%%', startangle=140, colors=colors)
plt.title("Estimated Distribution of Cyber Risk Types (Global Approximation)")
plt.axis('equal')  # Equal aspect ratio ensures that pie is drawn as a circle.
plt.tight_layout()
plt.show()

```

- **Python code for Figure (3): Severity of Financial and Operational Impacts of Cyber Risks**

```python
import matplotlib.pyplot as plt

# Define risk categories
risk_categories = [
    "Data Breach",
    "Ransomware Attack",
    "System Downtime",
    "Third-Party Vendor Failure",
    "Regulatory Non-Compliance",
    "Reputational Damage"
]

# Define severity levels (scale: 1 to 10)
financial_impact = [9, 10, 8, 7, 9, 6]
operational_impact = [8, 9, 10, 7, 8, 7]

# Set width of bars
bar_width = 0.35
x = range(len(risk_categories))

# Create bar chart
plt.figure(figsize=(12, 6))
plt.bar(x, financial_impact, width=bar_width, label='Financial Impact', color='darkred')
plt.bar([i + bar_width for i in x], operational_impact, width=bar_width, label='Operational Impact', color='navy')

# Labeling
plt.xlabel("Cyber Risk Categories")
plt.ylabel("Severity Level (1 = Low, 10 = High)")
plt.title("Severity of Financial and Operational Impacts of Cyber Risks")
plt.xticks([i + bar_width / 2 for i in x], risk_categories, rotation=45, ha='right')
plt.ylim(0, 11)
plt.legend()
plt.tight_layout()
plt.show()

```

- **Python code for Probabilistic Risk Modelling Approach**

```python
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt

# Set seed
np.random.seed(42)

# Simulation settings
num_simulations = 10000

# Define Egyptian market scenarios
scenarios = {
    "Optimistic": {
        "claim_frequency": 0.05,
        "claim_severity_mean": 50000,
        "claim_severity_std": 10000,
        "premium_multiplier": 1.3
    },
    "Moderate": {
        "claim_frequency": 0.1,
        "claim_severity_mean": 100000,
        "claim_severity_std": 20000,
        "premium_multiplier": 1.5
    },
    "Pessimistic": {
        "claim_frequency": 0.2,
        "claim_severity_mean": 200000,
        "claim_severity_std": 30000,
        "premium_multiplier": 1.7
    }
}

# Run simulations
results = []
for scenario, params in scenarios.items():
    claims = np.random.binomial(1, params["claim_frequency"], num_simulations)
    claim_costs = np.where(claims == 1, np.random.normal(params["claim_severity_mean"], params
    ["claim_severity_std"], num_simulations), 0)
    premiums = np.full(num_simulations, params["claim_severity_mean"] * params["premium_multiplier"])
    profits = premiums - claim_costs

    df = pd.DataFrame({
        "Scenario": scenario,
        "ClaimCost": claim_costs,
        "Premium": premiums,
        "Profit": profits
    })
    results.append(df)

results_df = pd.concat(results).reset_index(drop=True)

# Summary statistics
summary = results_df.groupby("Scenario").agg({
    "ClaimCost": "mean",
    "Premium": "mean",
    "Profit": ["mean", lambda x: np.mean(x < 0)]
}).round(2)
summary.columns = ["Mean Claim Cost", "Mean Premium", "Mean Profit", "Probability of Loss"]
print(summary)

# Plotting
plt.figure(figsize=(12, 6))
for scenario in results_df["Scenario"].unique():
    subset = results_df[results_df["Scenario"] == scenario]
    plt.hist(subset["Profit"], bins=50, alpha=0.6, label=scenario)

plt.title("Profit Distribution by Scenario")
plt.xlabel("Profit (EGP)")
plt.ylabel("Frequency")
plt.legend()
plt.grid(True)
plt.tight_layout()
plt.show()
```

- **Python code for Annual Cyber Losses Approach**

```python
import numpy as np
import pandas as pd
import matplotlib.pyplot as plt

# Set random seed
np.random.seed(42)

# Number of simulations and discount rate
n_simulations = 10000
discount_rate = 0.05  # 5% annual discount rate
years = 5  # projection period

# Scenario definitions
scenarios = {
    "Low Risk Org": {"mean_attacks": 0.5, "avg_loss": 30000, "premium": 19586.86},
    "Moderate Risk Org": {"mean_attacks": 1.5, "avg_loss": 50000, "premium": 97425.93},
    "High Risk Org": {"mean_attacks": 3.0, "avg_loss": 70000, "premium": 239049.83},
    "Tech Firm (High Severity)": {"mean_attacks": 1.0, "avg_loss": 150000, "premium": 122725.42},
    "Retail Chain (High Frequency)": {"mean_attacks": 5.0, "avg_loss": 25000, "premium": 162524.17},
}

results = []

for name, data in scenarios.items():
    annual_losses = []
    npv_profits = []

    for _ in range(n_simulations):
        yearly_profits = []
        for year in range(1, years + 1):
            # Simulate number of attacks
            num_attacks = np.random.poisson(data["mean_attacks"])
            losses = np.random.normal(loc=data["avg_loss"], scale=0.3 * data["avg_loss"], size=num_attacks)
            losses = np.clip(losses, 0, None)
            total_loss = np.sum(losses)

            profit = data["premium"] - total_loss
            discounted_profit = profit / ((1 + discount_rate) ** year)
            yearly_profits.append(discounted_profit)
        npv = np.sum(yearly_profits)
        npv_profits.append(npv)

        # Track year 1 for annual loss analysis
        if len(annual_losses) < n_simulations:
            annual_losses.append(data["premium"] - yearly_profits[0] * (1 + discount_rate))

    annual_losses = np.array(annual_losses)
    npv_profits = np.array(npv_profits)

    results.append({
        "Scenario": name,
        "Average Annual Loss": data["premium"] - np.mean(annual_losses),
        "Standard Deviation": np.std(annual_losses),
        "Expected Profit (Year 1)": np.mean(annual_losses),
        "NPV over 5 Years": np.mean(npv_profits),
        "Loss Probability Year 1 (%)": np.mean(annual_losses < 0) * 100,
        "Loss Probability NPV (%)": np.mean(npv_profits < 0) * 100,
        "Premium": data["premium"]
    })

# Save to Excel
df_results = pd.DataFrame(results)
df_results.to_excel("cyber_insurance_simulation_results.xlsx", index=False)

# Plotting
fig, axs = plt.subplots(2, 2, figsize=(14, 10))
fig.suptitle('Monte Carlo Simulation Results for Cyber Insurance Scenarios (5-Year NPV)', fontsize=16)

# NPV
axs[0, 0].bar(df_results['Scenario'], df_results['NPV over 5 Years'], color='purple')
axs[0, 0].set_title('NPV of Profit Over 5 Years')
axs[0, 0].set_ylabel('USD')
axs[0, 0].tick_params(axis='x', rotation=30)

# Loss Probability (Year 1)
axs[0, 1].bar(df_results['Scenario'], df_results['Loss Probability Year 1 (%)'], color='red')
axs[0, 1].set_title('Loss Probability (Year 1)')
axs[0, 1].set_ylabel('%')
axs[0, 1].tick_params(axis='x', rotation=30)

# Loss Probability (NPV)
axs[1, 0].bar(df_results['Scenario'], df_results['Loss Probability NPV (%)'], color='darkred')
axs[1, 0].set_title('Loss Probability (NPV over 5 Years)')
axs[1, 0].set_ylabel('%')
axs[1, 0].tick_params(axis='x', rotation=30)

# Expected Profit Year 1
axs[1, 1].bar(df_results['Scenario'], df_results['Expected Profit (Year 1)'], color='green')
axs[1, 1].set_title('Expected Profit (Year 1)')
axs[1, 1].set_ylabel('USD')
axs[1, 1].tick_params(axis='x', rotation=30)

plt.tight_layout(rect=[0, 0.03, 1, 0.95])
plt.savefig("cyber_insurance_simulation_chart.png")
plt.show()

```