FEDERATION OF AFRO-ASIAN INSURERS AND REINSURERS
F.A.I.R.

# FAIR Review

Issue No. 181 - Sep. 2019

# Kazakhstan

## Transitioned from lower-middle-income to upper-middle income status in less than two decades

- Cyber Insurance And Risk Management: Closing The Gap
- 1st FAIR Medical Insurance & Healthcare Congress Conference


Together ..
Towards Future
MISR INSURANCE
We meet all your needs
Energy , Aviation ,Engineering , Fire,Marine, Motor, Accident & Medical
call center 19114
www.misrins.com.eg

ISSN 1687-2231

# FAIR Review

## FAIR in Brief

Federation of Afro-Asian Insurers & reinsurers "FAIR" is a priceless instrument and media for cooperation, and our responsibility is to make it more responsive, more effective and more dynamic. FAIR was established in September 1964, to promote cooperation among insurance and reinsurance companies in Africa and Asia, through the regular exchange of information, experience and the development of business relations.

**Vision**:

FAIR aims to become a driving force international insurance cooperation by promting collaboration and adoption of international standards.

**Mission**:

FAIR will lead the effort to achieve harmonization of insurance markets by promoting the adoption and implementation of international standards among members facilitating the sharing of information and expertise and enhancing cooperation to be of added value to members.

**FAIR's added value is based on**:

- Wide recognition of brand and name of FAIR on the world scene,
- A broad range of deliverable affecting the members' interests,
- Strong national membership base,
- Extensive networking at both international and regional levels,
- Building regional bases (hub) that provides a variety of shared resources and services to local member companies.

## FAIR Review

The "FAIR Review" is published quarterly by the central office and circulated to Members free of charge. It is devoted to disseminate the research work, articles and information, to enhance professional knowledge among insurance professionals.



**Issue No. 181**
**Sep. 2019**



Contact us

129 ElTahrir St.,
Doqi, Giza - Egypt

Phone: (202) 37485429
37485436

Whatsapp : (20) 1099575725

review@fair.org.eg
www.fair.org.eg

Printed in: Toukhy Misr Printing
Tel.: +202 23935626

# Contents

# Global News

## • *Insurance Industry and Country Risk Assessments Under Our Revised Criteria*

S&P Global Ratings

Under its revised criteria for rating insurers (published July 1, 2019), S&P Global Ratings has assigned insurance industry and country risk assessments (IICRAs) to 97 insurance sectors, covering 48 countries and four global sectors.

An insurer's business risk profile forms one of the key components of our rating analysis. It measures the risk inherent in the insurer's operations, which affects the sustainable return that may be derived from those operations. The business risk profile is based on our analysis of an insurer's competitive position, modified to incorporate the industry and country risks to which a specific insurer is exposed.

Each IICRA addresses the risks typically faced by all the insurers that operate in a specific industry and country. To determine the IICRA, we apply our "Country Risk Assessment Methodology And Assumptions," published on Nov. 19, 2013, to assess country risk, and then modify it according to our view of industry risk. We assess country risk on a scale from strongest (very low risk) to weakest (very high risk).

We assess industry risk on a four-point scale from low to high. Our analysis of industry risk addresses the level, volatility, and sustainability of profitability in a given industry sector. The primary factor in our industry risk analysis is an assessment of prospective profitability, supplemented by a holistic analysis of factors that in combination are likely to either support or threaten industry profitability prospects, such as barriers to entry, market growth prospects, product risk, and the institutional framework.

The impact of IICRAs on our ratings varies according to the degree of risk. The higher the risk, the greater the adverse impact on the business risk profile. The risks are categorized as 1-very low, 2-low, 3-intermediate, 4-moderately high, 5-high, or 6-very high.

Within each country, if applicable, we separately assess the life sector and the property/casualty (P/C) sector. Where it has a distinct legal and regulatory framework, we also assess the health sector separately. In addition, in certain countries, we assess the insurance industry and country risk for the bond, mortgage, and title insurance sectors.

Some sectors are more naturally global, because insurers in those sectors typically write business in multiple countries around the world. Consequently, we assess IICRAs on a global basis for life reinsurance, P/C reinsurance, trade credit insurance, and marine protection and indemnity insurance.

We expect to update our reports on all of the sectors listed below over the next 12-18 months. In the interim, the rating rationales we release on each insurer will show how the IICRA affects our ratings.

The geographical spread of our life and P/C IICRAs and the level of risk we see in each country are shown in charts 1 and 2. All the IICRAs are listed, by sector and country, in the table next.

**Chart 1**
**Insurance Industry And Country Risk Assessment: Property And Casualty**

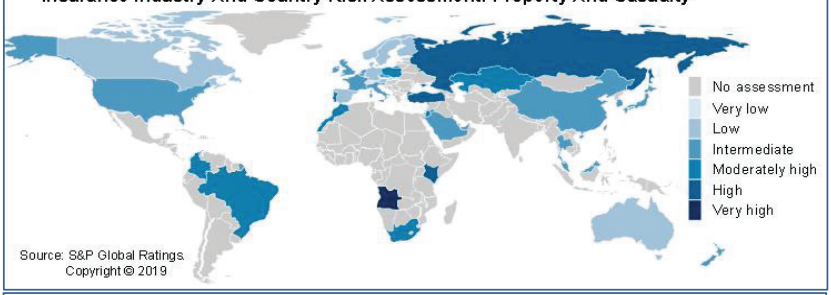
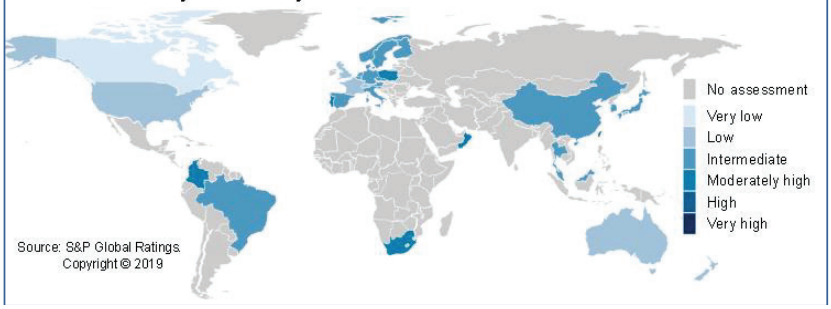



**Chart 2**
**Insurance Industry And Country Risk Assessment: Life**




## Insurance Industry and Country Risk Assessments

### Property/casualty sector

| Country | Assessment | Country | Assessment |
|---|---|---|---|
| Angola | 6 - Very high | Kuwait | 3 - Intermediate |
| Australia | 2 - Low | Malaysia | 3 - Intermediate |
| Austria | 2 - Low | Morocco | 4 - Moderately High |
| Bahrain | 4 - Moderately High | Netherlands | 3 - Intermediate |
| Belgium | 3 - Intermediate | New Zealand | 3 - Intermediate |
| Brazil | 4 - Moderately High | Norway | 2 - Low |
| Canada | 2 - Low | Poland | 4 - Moderately High |
| China | 3 - Intermediate | Portugal | 4 - Moderately High |
| Colombia | 4 - Moderately High | Qatar | 3 - Intermediate |
| Czech Republic | 3 - Intermediate | Russia | 5 - High |
| Denmark | 2 - Low | Saudi Arabia | 3 - Intermediate |
| Finland | 2 - Low | Singapore | 2 - Low |
| France | 3 - Intermediate | Slovenia | 3 - Intermediate |
| Germany | 2 - Low | South Africa | 4 - Moderately High |
| Hong Kong | 2 - Low | Spain | 2 - Low |
| Ireland | 3 - Intermediate | Sweden | 2 - Low |
| Israel | 3 - Intermediate | Switzerland | 1 - Very Low |
| Italy | 3 - Intermediate | Taiwan | 3 - Intermediate |
| Japan | 3 - Intermediate | Thailand | 3 - Intermediate |
| Jordan | 4 - Moderately High | Turkey | 5 - High |
| Kazakhstan | 4 - Moderately High | United Arab Emirates | 3 - Intermediate |
| Kenya | 5 - High | U.K. | 3 - Intermediate |
| Korea | 3 - Intermediate | U.S. | 3 - Intermediate |

## Life sector

| Country | Assessment |
|---|---|
| Australia | 2 – Low |
| Austria | 3 - Intermediate |
| Belgium | 3 - Intermediate |
| Brazil | 3 - Intermediate |
| Canada | 1 - Very Low |
| China | 3 - Intermediate |
| Colombia | 4 - Moderately High |
| Czech Republic | 3 - Intermediate |
| Denmark | 3 - Intermediate |
| Finland | 3 - Intermediate |
| France | 2 - Low |
| Germany | 3 - Intermediate |
| Hong Kong | 2 - Low |
| Israel | 3 - Intermediate |
| Italy | 3 - Intermediate |
| Jamaica | 5 - High |
| Japan | 3 - Intermediate |
| Korea | 3 - Intermediate |

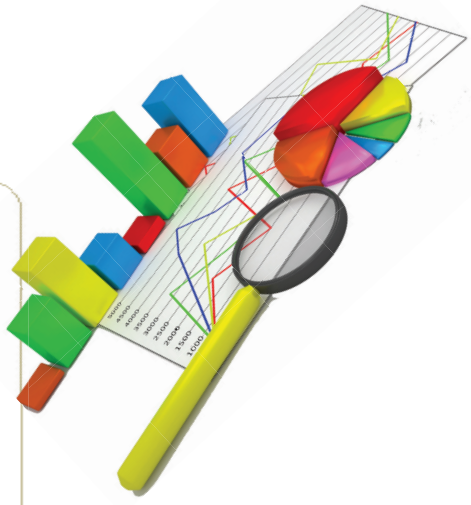
| Country | Assessment |
|---|---|
| Malaysia | 3 - Intermediate |
| Netherlands | 3 - Intermediate |
| New Zealand | 2 - Low |
| Norway | 3 - Intermediate |
| Oman | 4 - Moderately High |
| Poland | 4 - Moderately High |
| Portugal | 4 - Moderately High |
| Singapore | 2 - Low |
| Slovenia | 3 - Intermediate |
| South Africa | 4 - Moderately High |
| Spain | 3 - Intermediate |
| Sweden | 3 - Intermediate |
| Switzerland | 2 - Low |
| Taiwan | 4 - Moderately High |
| Thailand | 3 - Intermediate |
| U.K. | 2 - Low |
| U.S. | 2 - Low |

## Health sector

| Country | Assessment |
|---|---|
| Australia | 2 - Low |
| Brazil | 4 - Moderately High |
| Germany | 3 - Intermediate |
| Netherlands | 3 - Intermediate |
| New Zealand | 3 - Intermediate |
| South Africa | 4 - Moderately High |
| U.S. | 2 - Low |

| Global sectors | |
|---|---|
| Global life reinsurance | 2 - Low |
| Global marine protection & indemnity | 3 - Intermediate |
| Global property/casualty reinsurance | 3 - Intermediate |
| Global trade credit | 3 - Intermediate |

| Other sectors | |
|---|---|
| Australia mortgage insurance | 2 - Low |
| Canada mortgage insurance | 2 - Low |
| U.S. mortgage insurance | 3 - Intermediate |
| U.S. bond insurance | 2 - Low |
| U.S. title insurance | 2 - Low |

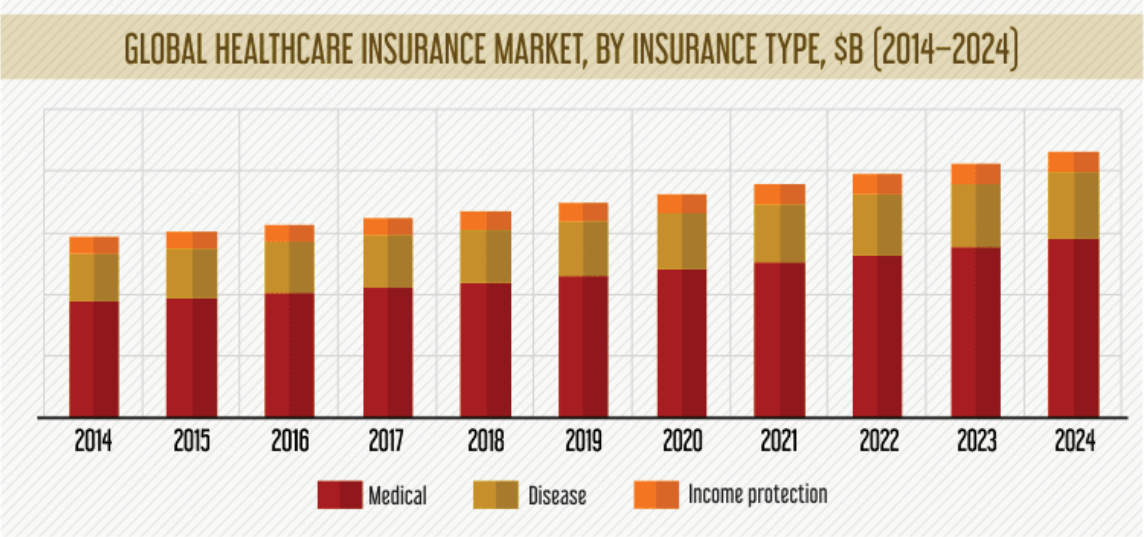


S&P Global
Ratings

Source: S&P Global Ratings | 5 July 2019

## • *Healthcare Insurance Market*

By Prescient & Strategic Intelligence Private Limited – March 2019




According to the report, the global healthcare insurance market is predicted to attain a size of $2.2 trillion by 2024, progressing at a CAGR of 4.3% during the forecast period (2019–2024). The main factors driving the growth of the market are increasing prevalence of chronic diseases, surging geriatric population, rising healthcare expenditure, and huge medical costs around the globe.

Lifetime and term are the two kinds of coverages offered in the global healthcare insurance market. In 2018, the term coverage category held the larger revenue share of 76.5% in the market. This can be ascribed to various benefits attached with this category, such as receipt of a lump sum amount at term end, low cost of premiums, and rising awareness about the advantages of health insurance among the global population.

The service provider segment is classified into private and public. Of these, the public service provider classification dominated the healthcare insurance market. In 2018, it generated a revenue of nearly $0.9 trillion and is projected to reach $1.2 trillion by 2024, advancing at a CAGR of 4.1%. However, the private service provider classification is anticipated to observe the faster growth in the market, registering at a CAGR of 4.7% during 2019–2024.

North America is leading the global healthcare insurance market and is projected to advance at a CAGR of 3.7% during the forecast period, owing to the well-structured insurance and healthcare system, compulsory provision of health insurance from employers, and increasing number of chronic disease cases in the continent.

The USA has the largest health care system in the world and one of the biggest health insurance markets and spends

PRESCIENT & STRATEGIC INTELLIGENCE
Where knowledge inspires strategy


more than 16% of its GDP on health care. Private health insurance alone is an $884-billion industry. According to the trade association America's Health Insurance Plans (AHIP), about 90% of insured Americans are enrolled in healthcare plans by managed care organizations and UnitedHealth Group Inc., Anthem Inc. and Humana Inc. are the leading players in this.

The US industry is being impacted by the Patient Protection and Affordable Care Act (PPACA), colloquially Obamacare, a US law aimed at reforming the American health care system. The PPACA was enacted to increase the quality and affordability of health insurance, lower the uninsured rate by expanding public and private insurance coverage, and reduce the costs of healthcare for individuals and the government.

Asia share of the global health cover industry is small, but the market is growing due to the increasing popularity of health insurance products and rising disposable incomes. China, Japan and India are the largest health insurance markets. Asian healthcare spending is expected to grow to more than $2,000 billion over the next few years. Low levels of public funding coupled with the increasing cost of healthcare are expected to create an expanding market for voluntary health insurance. China Life Insurance Company Limited, GlobalHealth Asia International Group and United India Insurance Company Limited are among the largest companies in this market.

On a global ground, the market is predicted to observe the fastest growth in Asia-Pacific (APAC), registering a CAGR of 5.7% during the forecast period. Furthermore, the region is estimated to generate a revenue of nearly $0.5 trillion for the market by 2024. The main factors driving the market growth in APAC are expanding healthcare sector, growing healthcare awareness, and increasing prevalence of chronic diseases.

European health cover is mainly supplied by governments and therefore private health care spending and growth are low in most European countries. AXA PPP, Aviva plc and BUPA Health Insurance are some of the companies in this industry.

Australia spends about 6% of its GDP on healthcare. Most funding is provided by the state through Medicare. Over the past decade the Australian government has encouraged consumers to buy private health insurance to help reduce Medicare costs; however, there has been no substantial growth in this. Currently the country has 36 private health care funds; the largest is Medibank Private, which accounts for about 33% of the market.

## Market Outlook

Key trends in the health insurance industry concern increasing life expectancy and wealth.

- Life expectancy is expected to increase to about 73 years in the near future, bringing the number of people over age 65 to around 700 million worldwide. The aging population is likely to create additional demand for health care services in the future.
- Concurrently, the number of high income households (those earning over $25,000 per year) is expected to increase by about 10%, with over one half of that growth coming from Asia. Together these two trends are likely to contribute to the growth in the industry which is forecast to reach more than $800 billion in the near future.
- Starting in 2018, Americans with high-cost health insurance through their employers will have to pay a 40% excise tax known as the Cadillac tax on their policies. The tax will apply to employer-sponsored policies with premiums higher than $27,500 for a family or $10,200 for an individual. The purpose is to reduce excess health care spending by employees and employers and help finance the expansion of health coverage under the PPACA. This tax may reduce the size of the US market. ■

## • *London market issues cyber risk exclusion clauses to tackle silent cover*


New model exclusion clauses have been issued by the London market to make it easier for insurers to exclude cyber risks from traditional lines of cover.

The clauses are in response to growing concern from insurers over silent or non-affirmative cyber cover in other lines of business. They are also a response to regulatory pressure.

Publishing two exclusion clauses, the International Underwriting Association (IUA) said the wordings are needed to remove "uncertainty" over insurance covering unintended cyber risks. It argues they will make things clearer for insurance buyers.

The Cyber Loss Absolute Exclusion Clause will allow underwriters to broadly exclude any losses arising from a computer system, network or data. The second Cyber Loss Limited Exclusion Clause will exclude only losses directly caused by cyber events.

Chris Jones

Chris Jones, IUA director of legal and market services, said: "These two new model clauses provide broad policy exclusions, which may be utilised as a starting or reference point for underwriters offering cover for traditional business classes that may include an element of cyber risk. By developing class-specific writebacks, insurers can then explicitly state the extent of any cover provided for such losses."

BANK OF ENGLAND
PRUDENTIAL REGULATION AUTHORITY

UK regulator the Prudential Regulation Authority (PRA) first raised concerns about unintended cover for cyber risks in November 2016.

In July 2017, it issued Supervisory Statement SS4/17, setting out its views on silent cyber cover. This considered how traditional insurance policies can respond to cyber losses even where this is not the intention of the insurer.

The statement marked a gearchange in regulatory oversight from the PRA, which is now encouraging insurers to clarify where and to what extent cyber cover is provided in insurance policies. The PRA's supervisory statement called on insurers to identify silent cyber exposures and to accordingly adjust premiums, limits and/or use "robust wordings". The PRA also called on insurers to produce cyber risk appetite statements and increase their cyber technical expertise.

Mr Jones said the insurance industry has been working on tightening wordings to better manage exposure to cyber risks. Several leading global insurers have announced individual plans to do just that.

"Silent cyber cover creates uncertainty for both insurers and clients and has been a hot topic in the London company market for some time now. Increasing regulatory scrutiny has, of course, further highlighted the issue, but IUA members have been considering different approaches even before it was first raised by the PRA," said Mr Jones.

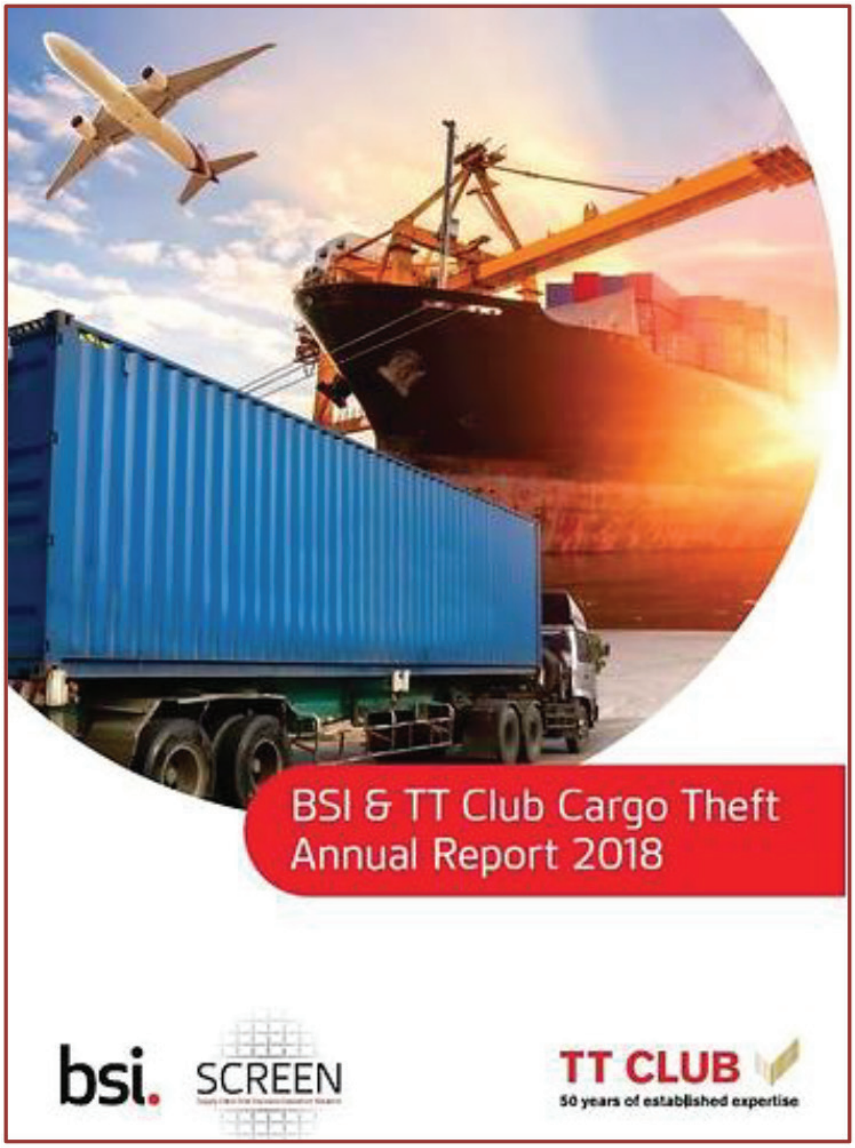
"Many traditional policies were designed when cyber wasn't a major risk and often do not explicitly mention cyber.

**Speaking to CRE last year when model IUA cyber clauses were in the pipeline, Mr Jones said clarifying silent cyber exposures appeared to be the direction of travel for insurers.**

Underwriters of traditional lines are increasingly likely to exclude silent cyber exposures, but provide affirmative cover where appropriate, he said. Exclusions should also raise awareness of broader or more specialist cover being made available in the standalone cyber insurance market, such as cover for data breaches and contingent cyber business interruption, said Mr Jones. ■

Source: Commercial Risk Online - 6 June 2019

## • *Cargo theft loss prevention must focus on insider threat:* Report




Theft from trucks continues to account for the highest proportion of cargo thefts worldwide and the threat from insiders – employees, contractors and even business partners – continues to rise, according to analysis carried out by transport insurer TT Club and supply chain intelligence firm BSI.

**The Global Cargo Theft Intelligence Report for 2018** found that thefts from trucks accounted for 84% of incidents worldwide.

By theft type, slash and grab accounted for 26%, hijackings came second on 16% and theft from truck on 12%.

In Europe, a lack of secure parking for trucks coupled with mandatory breaks for drivers after certain time periods means that trucks and their drivers are particularly vulnerable.

Based on the analysis, the UK accounts for a massive 84% of thefts in Europe, with

Germany on 4% and Italy with 3% of the total.

The most commonly targeted goods are food and beverage (15%) and alcohol and tobacco (also 15%), with consumer products next on 13%.

By location, in-transit accounted for 29%, rest area 16%, warehouse 11% and unsafe roadside parking 11%.

South America tops the median value chart, with $77,000 per theft and

Brazil accounting for 68% of the total. Next comes Europe at $59,866 per theft.

North America comes third at $58,500 per theft and with Mexico accounting for 68%.

Middle East and Africa came in at $40,000 per theft, with South Africa (31%) and Egypt (31%) leading the way.

The median value per theft in Asia is $18,923, with India accounting for 59% of thefts and China 24%.

The insider threat is a real problem in Asia, as worldwide.

"Supply chain corruption is a major element of theft in India and China, with corrupt employees removing goods they are transporting or accessing shipments in warehouses or logistics facilities," states the report.

"People are an organisation's biggest asset; however, in some cases they can also pose an insider risk.

As organisations implement increasingly sophisticated physical, procedural and cybersecurity measures to protect their assets from external threats, the recruitment of insiders becomes a more attractive option for those attempting to gain access," it adds.

"An insider could be a full-time or part-time employee, a contractor or even a business partner.

An insider could deliberately seek to join an organisation to conduct an insider act, or may be triggered to act at some point during their employment.

Employees may also inadvertently trigger security breaches through ignorance of rules, or deliberate non-compliance (due to pressure of work)," the report notes.

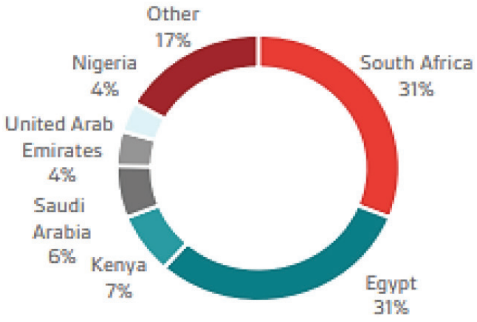
*The report states that studies indicate there are five main types of insider activity:*

- Unauthorised disclosure of sensitive information
- Process corruption
- Facilitation of third-party access to an organisation's assets
- Physical sabotage
- Electronic or IT sabotage.

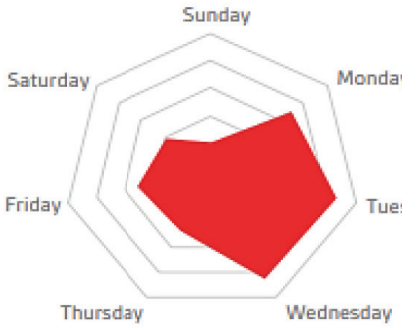
The most frequent types of insider activity identified are unauthorised disclosure of sensitive information (47%) and process corruption (42%).

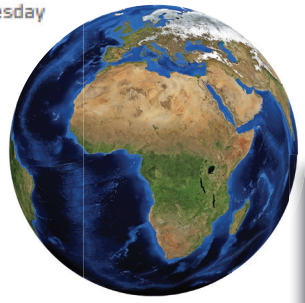
# Middle East and Africa

### Top Countries for Cargo Theft

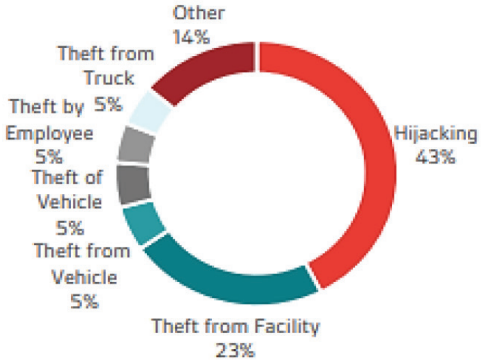



### Cargo Theft by Day

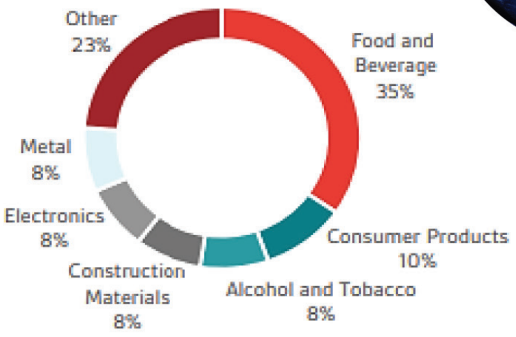


### Type of Cargo Theft

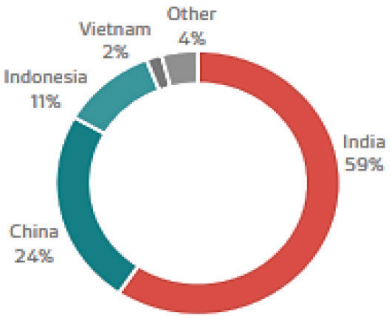



### Top Commodities Stolen

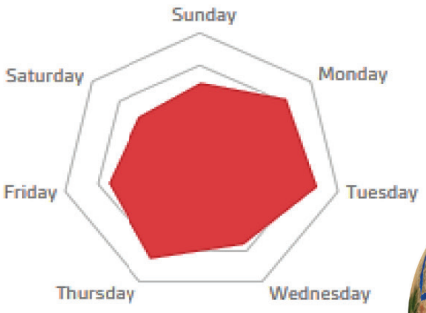


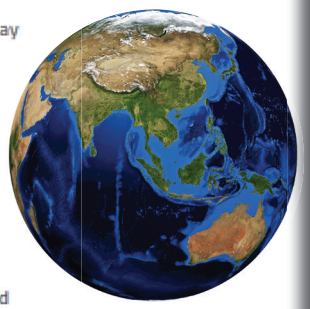

# Asia

### Top Countries for Cargo Theft

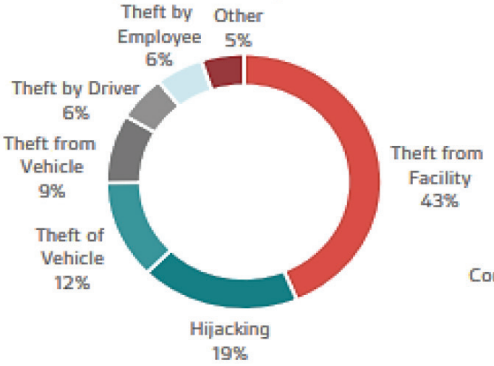



### Cargo Theft by Day

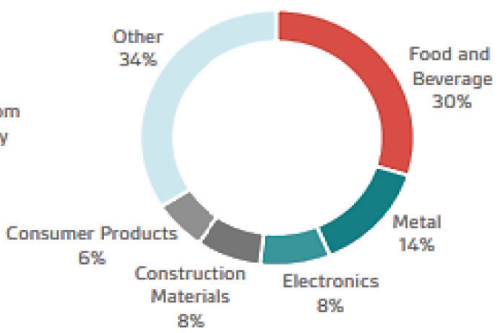


### Types of Cargo Theft

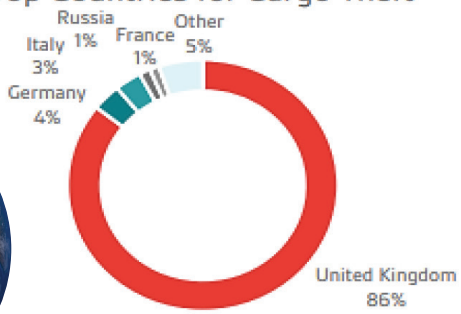



### Top Commodities Stolen

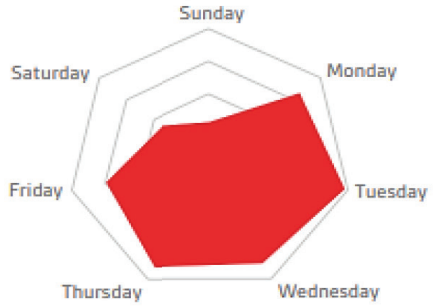


# Europe

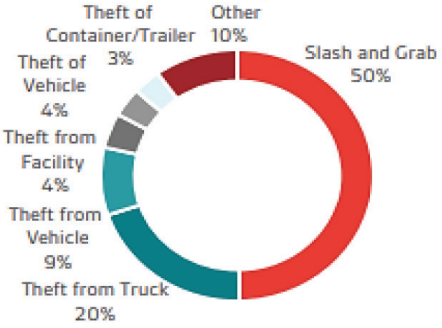
## Top Countries for Cargo Theft



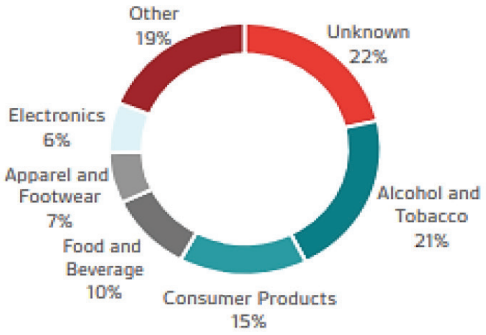

## Cargo Theft by Day




## Type of Cargo Theft

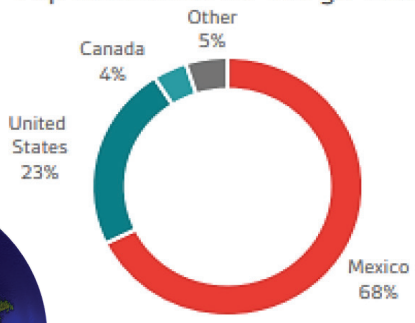



## Top Commodities Stolen

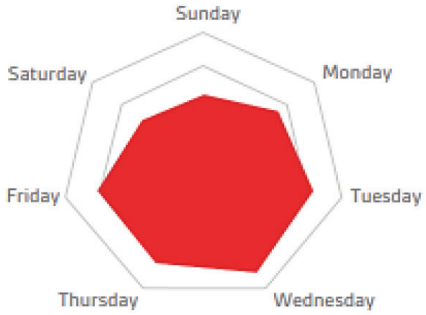



# North America

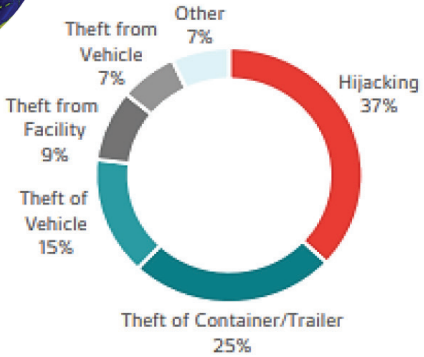
## Top Countries for Cargo Theft



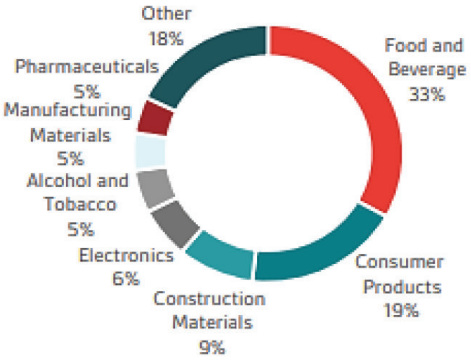

## Cargo Theft by Day




## Cargo Theft Type

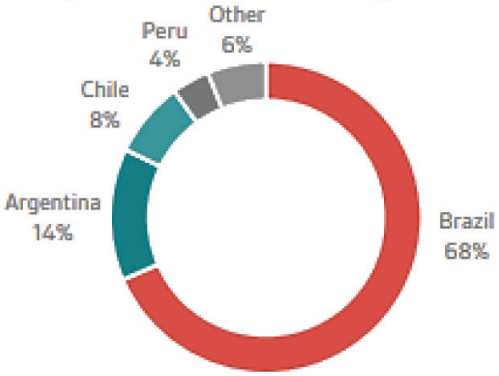



## Top Commodities Stolen

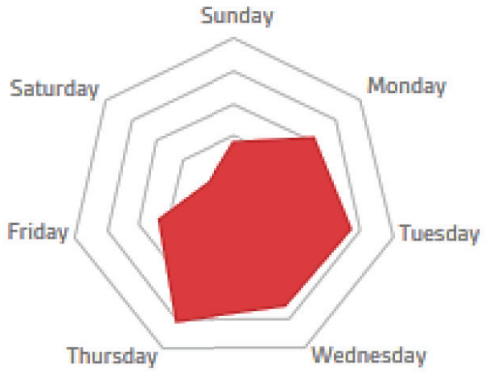


# South America

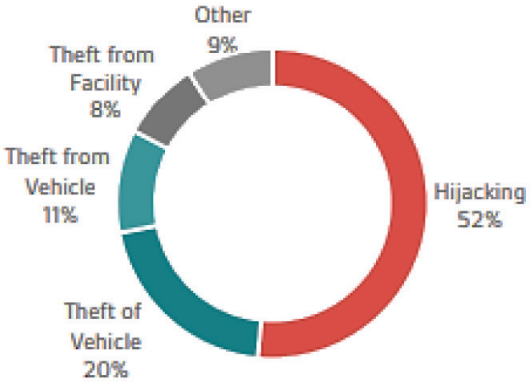
## Top Countries for Cargo Theft



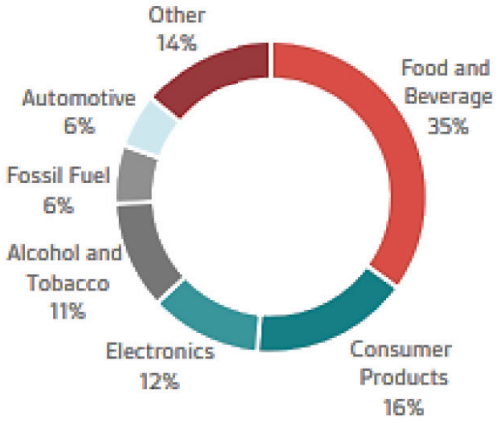

## Cargo Theft by Day

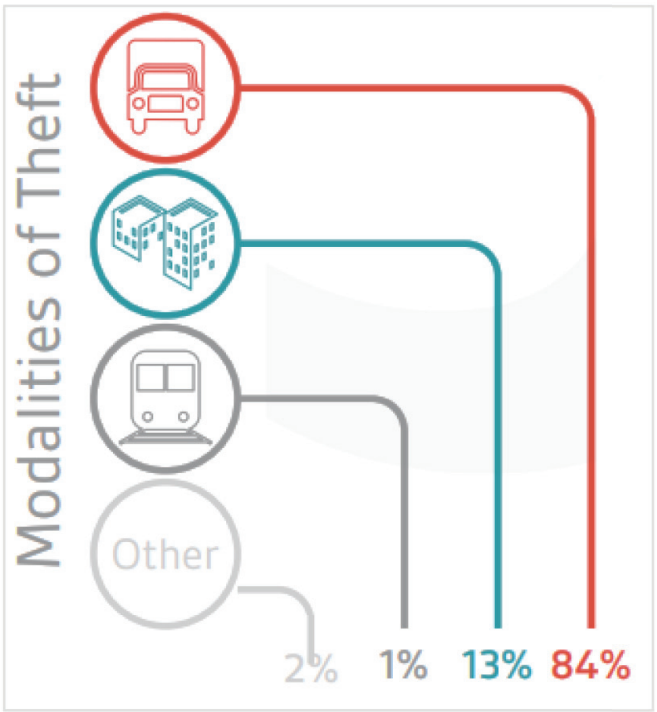



## Cargo Theft Type




## Top Commodities Stolen




Source:
BSI & TT Club Cargo Theft Report
& Commercial Risk Online – 18 June 2019


# FAIR

## Non-Life Reinsurance Pool

Since 1974 under the management of Milli Re

### Classes of Business Accepted by the Pool:

- Fire
- Accident
- Engineering (including C.A.R., E.A.R. and M.B.)
- Marine Hull and Cargo

MİLLİ RE

Milli Reasürans T.A.Ş.
Teşvikiye Caddesi No: 43-57 34367 Teşvikiye ISTANBUL / TURKEY
Phone: +90 (212) 231 47 30 Fax: +90 (212) 230 86 08
www.millire.com.tr

# Africa News

## ANGOLA

### • *Importers compelled to underwrite local marine insurance policy*

The Angolan government is intent on introducing a law requiring from importers to underwrite a local marine insurance policy and to pay the relevant premiums in local currency. This regulation has been designed to reduce local currency exit and recourse to foreign insurers.

It is worth noting that Angola is currently sustaining budget deficit and drastic shrinking of its exchange reserves. This situation is accounted for by the fluctuating oil prices, a sector that represents 95% of exchange revenues and 40% of GDP. ■

# CAMEROON

## • Evolution of turnover per Non-Life insurance company (2012-2016)

*in USD*

| | 2012 | 2013 | 2014 | 2015 | 2016 | 2016 shares |
|---|---|---|---|---|---|---|
| AXA Assurances | 22532093 | 25905881 | 25269501 | 32452270 | 32867791 | 15.5% |
| SAAR Assurances | 29649709 | 38695302 | 34008882 | 29958984 | 30423877 | 14.4% |
| ACTIVA Assurances | 28401580 | 31605455 | 28670468 | 27773270 | 28461664 | 13.5% |
| Allianz Assurances Cameroun | 19643332 | 20820812 | 19506914 | 21562164 | 21546254 | 10.2% |
| Chanas Assurances | 47009763 | 42911095 | 35667441 | 24101914 | 18766754 | 8.9% |
| Garantie Mutuelle des Cadres | 11146460 | 15497882 | 14330289 | 15061143 | 15027814 | 7.1% |
| Zenithe Insurance | 6113803 | 11849442 | 7465153 | 13091230 | 12374920 | 5.9% |
| NSIA Assurances | 16159348 | 19180002 | 12010799 | 11867341 | 12047895 | 5.7% |
| Saham Assurances Cameroun | 15702446 | 13940190 | 6819903 | 12420758 | 11412626 | 5.4% |
| Assurances & Réassurances Africaines (AREA) | 4425063 | 5370056 | 7030209 | 6817159 | 6390272 | 3% |
| Compagnie Professionnelle d'Assurances (CPA) | 4317747 | 3986946 | 4118955 | 4691128 | 4711623 | 2.2% |
| Assurances Générales du Cameroun | 3534622 | 5088139 | 5208670 | 4434385 | 4120032 | 2% |
| Pro Assur | 3031479 | 4144120 | 3878497 | 3992056 | 3971818 | 1.9% |
| Beneficial General Insurance | 2858801 | 3343536 | 2949362 | 2579312 | 3561405 | 1.7% |
| Cameroon Insurance (CAMINSUR) | 2535680 | 3078869 | 3346058 | 3619195 | 2838952 | 1.3% |
| Samaritan Insurance | 5515906 | 5731734 | 6684808 | 3242096 | 2737592 | 1.3% |
| **Total** | **222577832** | **251149461** | **216965909** | **217664405** | **211261289** | **100%** |

## • Premiums 2018 of the Cameroonian insurance market

YaoundéThe total premiums' volume achieved by the Cameroonian insurance market reached 205 billion FCFA (356 million USD) in 2018 compared to 161 billion FCFA (338 million USD) in 2013, that is an increase of 27.4% over five years. However, the insurance penetration rate remains low, of less than 2%.

These figures were revealed by Théophile Gérard Moulong, General Manager of Saham Assurances, during the 2nd edition of "the insurance day", which is being held from 29 May to 1 June in Douala. This low penetration rate goes hand in hand with a very high level of non-insurance, even for compulsory covers sucg as motor third party liability . According to the ASAC President, less than 40% of vehicles are insured in Cameroon

The company's overall investments amounted to 370.8 billion FCFA (645 million USD) in 2018, representing 2.1% of GDP. ■

Sources: Atlas Magazine – 30 January 2018 &12 June 2019

# CÔTE D'IVOIRE

## • The Ivorian insurance market in 2018

The Côte d'Ivoire's association of insurance companies (ASA-CI) has published the figures of the insurance sector for 2018.

The market reported a turnover of 360.2 billion FCFA (628 million USD) increasing by 9.3% compared to 329.2 billion FCFA (601 million USD) in 2017.

The non-life class totalizes 205 billion FCFA (359 million USD) in premiums which represents a 57% market share. The life activity records 154.6 billion FCFA (270 million USD) which corresponds to 43% of market shares.

For 10 years now, the growth rate of nearly 8% has been consistent. Nevertheless, the Ivorian insurance market records a low penetration rate and this is notably due to the bad reputation of insurers. According to the Ivorian population, these latter considerably delay their motor claim settlements. ■

Source: Atlas Magazine - 25 June 2019

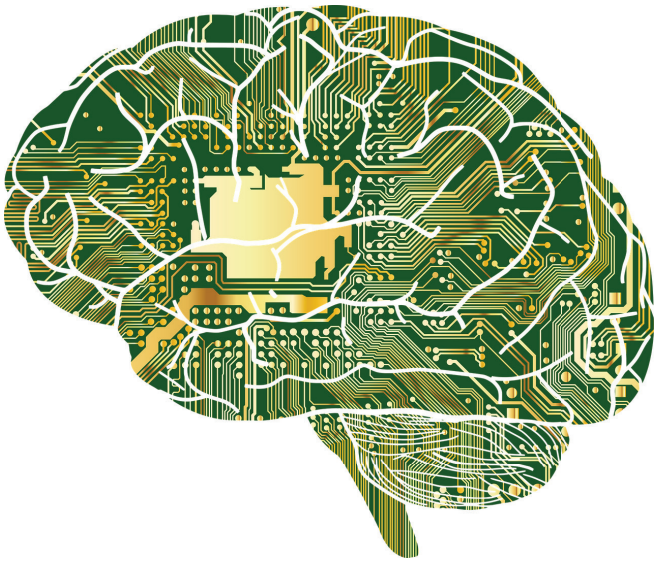
## • Creation of a new insurance platform in Côte d'Ivoire

Being the fruit of a public-private partnership, the newly created Ivorian company of digital intelligence (SIIN), unveiled on the 21st of June 2019 its online subscription platform «Easy Assur».

Dedicated to claims management and insurance products marketing, the portal provides users with home, motor, travel and personal accident insurance policies. Other products such as life insurance shall be presented later.

Easy Assur will be launched in June 27th, 2019. The project has already received the approval of the Directorate General of the Treasury and Public Accounting as well as that of The Côte d'Ivoire's association of insurance companies (ASA-CI). ■

Source: Atlas Magazine – 25 June 2019



# EGYPT

## • *Central bank plans to launch export credit insurer targeting Africa*

The Central Bank of Egypt (CBE) is preparing to launch a risk insurance company for exports to Africa before the end of this year, Mr Ramy El-Shaarawy, general department head, banking reform sector, at the bank.

Ramy El-Shaarawy

Mr El-Shaarawy told Daily News Egypt that the bank is currently completing the regulatory and structural framework of the new company, determining shareholders' stakes, and the CBE's contribution to the company.

He added that there are several sectors, such as electrical appliances and garments, that can compete in the African market.

Ms Naglaa Nozahie, CBE governor's advisor for African affairs and supervisor of the economic research sector, has said that intra-Africa trade currently stands at 17%, compared to intra-EU trade of 85%.

In March, she said at an economic forum that the CBE had finished the first phase of studies to establish an export credit guarantee company to insure and finance Egyptian exports into the African market. The plans are for the export credit insurer to provide trade receivables management solutions ranging from trade credit insurance to credit information, debt collection and trade finance. ■

Source: Middle East Insurance review (MEIR) - 4 July 2019


# YOUR CONVENICE IS OUR GOAL

**MLI App** Fast and easy way of effectively managing your insurance

GET THE APP

App Store | Google Play

misr_life_ins | misrlifeinsurance

www.misrlife.com / call 19446

MISR LIFE INSURANCE

TOMORROW STARTS TODAY

مصر القابضة للتأمين
MISR INSURANCE HOLDING COMPANY

وزارة قطاع الأعمال العام

# NIGERIA

## • *Insurance market sees premiums jump by 10% in 2018*

Premium income in the Nigerian insurance sector rose by 10% to NGN400bn ($1.1bn) in the 2018 financial year, according to the Nigerian Insurers Association (NIA).

NIGERIAN INSURERS ASSOCIATION
...the trade association of insurance and reinsurance companies in Nigeria

NIA chairman Mr Tope Smart, presenting the 2018 annual report of the Nigerian insurance sector recently, said, "During the year under review, the volume of business written by member companies grew from NGN363bn in 2017 to about NGN400bn in 2018."

Tope Smart

He said the Nigerian insurance sector continued to take pride of place in the economic space as the livewire of the larger national economy. However, he also outlined several economic and socio-political problems facing the country during the past year.

According to a report by Economic Confidential, he said, "Power outages continue to be a major challenge to businesses; failure to abolish or amend CITA (Companies Income Tax Act) 2007 remains a huge burden for insurance companies; growing herdsmen/farmers' clashes across the country; insurgency and armed banditry in the North; rising cases of kidnapping; armed robbery and other violent crimes as well internecine communal clashes in some states, all combined to negatively affect the bottom line of many insurance companies."


He said despite the challenges, insurance companies continued to discharge their obligations to the insured in line with their mandate.

Mr Smart said the association was working closely with the industry regulator, the National Insurance Commission, to promote the business of insurance and increase its contribution to the economy.

"Some of these initiatives include the insurance industry rebranding project, regulations on microinsurance, collaboration on financial inclusion bancassurance guidelines and others, which will impact positively on the business of insurance companies," he added.

As at 31 December 2018, the total assets of the Nigerian financial sector, consisting of banking, pensions and insurance, stood at $110bn, of which the share of the insurance sector was less than 3%.■

Source: Middle East Insurance Review | 15 July 2019

# SUDAN

## • *Insurance companies are preparing for huge claims from riots*

Sudanese insurance companies are currently preparing to pay compensation to policyholders that are expected to be millions of Sudanese pounds, according to an industry estimate.

The claims arise from losses incurred in deadly riots and confrontation with government militias in June. The payouts are to be made to those with riot cover. Insurance policies that cover riots and disturbances are bought as a rider to fire insurance.

Sudanese loss adjusting companies licensed by the National Insurance Supervisory Authority have been activated. Insurance companies rely on them to estimate the losses and damages that have occurred and then recommend the amount of compensation.

Ms Halima Nial, director of licensing at the National Insurance Supervision Authority of the Ministry of Finance and Economic Planning in Sudan, told Asharq Al-Awsat that insurance companies would not face the risk of bankruptcy. All companies have agreements with global reinsurance companies, she said.

Major entities in the country, such as the Union of Sudanese Banks, the University of Khartoum and major companies, especially telecommunications companies, have completed their loss assessments. For instance, the University of Khartoum estimated its losses in billions of Sudanese pounds. Others estimate losses of between SDG10m ($221,000) to SDG40m each for small and medium-sized businesses, which overlook the main streets of Khartoum.

The National Insurance Supervisory Authority, which monitors and licenses local and foreign companies in Sudan, has not yet received details of the extent of losses sustained by the State, individuals and companies as a result of the protests. ■

MIDDLE EAST INSURANCE REVIEW

3 July 2019

# TANZANIA

## • Bancassurance Guidelines 2019

by Peter Kasanda, Michaela Marandu, Tenda Msinjili and Jasper Dymoke (Clyde & Co)

CLYDE&CO

In this month's banking updater, we review the Bancassurance Guidelines for Banks and Financial Institutions (the Guidelines) which were published on 13 May 2019. This updater should be read in conjunction with our updater of May 2019 in which we reviewed the Insurance (Bancassurance) Regulations (the Regulations).

As the Tanzanian insurance sector continues to expand and develop, there has been a concerted effort from the Tanzanian government to enable this growth in a coordinated and regulated manner. The inclusion of banks and financial institutions in the Bancassurance business provides significant opportunities for both the banking and insurance sectors in Tanzania.


In order to encourage banks and financial institutions to market insurance products and services in a manner that protects operators and consumers alike, guidelines have been produced by the Bank of Tanzania in order to provide banks and financial institutions confidence to enter a market in which regulation is necessary.

### Highlights of the Guidelines

Below are some key highlights of the Guidelines:

In order to engage in Bancassurance business, a bank or financial institution must obtain approval from the Bank of Tanzania and a licence from the Tanzania Insurance Regulatory Authority. In seeking this approval, a bank or financial institution must submit certain bits of key information to the Bank of Tanzania, and other information as may be necessary.

- In its consideration of granting approval to engage in Bancassurance business, the Bank of Tanzania shall consider a number of factors, including:
  * Whether the bank or financial institution meets the minimum legal and regulatory capital requirements
  * The viability of the Bancassurance business plan
  * The adequacy of the risk assessment and accompanying mitigants
  * The ability of the bank or financial institution to conduct Bancassurance business in a prudent manner
- Any amendment to a Bancassurance agreement must be approved by the Bank of Tanzania. This includes amendments to a Bancassurance Agency Agreement which is a legal contract between a bank or financial institution and an insurer, under which the former acts as the insurance agent of the latter.
- There are a number of reporting requirements for banks or financial institu-

tions engaged in Bancassurance business:

* Quarterly returns on the performance of the Bancassurance business must be submitted to the Bank of Tanzania one month after the end of each quarter
* Notes to annual financial statements must disclose the income and expenses associated with the provision of the Bancassurance business

## Operational requirements

The Guidelines also propose how banks and financial institutions should operate to regulate and maximise success in the insurance sector. The purpose here is to ensure that customers are suitably informed of the products available to them. As such, staff are expected to have the requisite training to enable them to explain the key attributes of insurance products and should be aware of the risk of misrepresentation and misleading statements when selling such products.

The Guidelines are explicit about what should be standard expectations of a non-insurer entity marketing insurance services. For example, a bank or financial institution must make it known that it does not underwrite risk or act as an insurer in any capacity whatsoever, as well as the need to inform the customer of the premium being charged.

## Consumer protection

Supporting the theme of consumer protection that was established in the Regulations with the ban of tied-selling, the Guidelines lay out a number of measures to safeguard the interests of consumers. These are typical of an entity marketing insurance products, ranging from confidentiality obligations to the need to avoid customer coercion.

Whilst there has always been collaboration between the banking and insurance sectors, it will be interesting to see how both sectors work together to take advantage of what is a fast developing business, whilst at the same time, maintaining an awareness of the need to protect consumers. As such, simple compliance measures have been put in place to ensure their interests are not jeopardised. For example, banks and financial institutions must not offer different rates to those offered by the insurer and must be cautious when it comes to branding, ensuring that insurance documents are not branded by the bank or financial institution's name, logo or corporate colours.

## Sanctions

Should the Guidelines not be adhered to, the Bank of Tanzania has the authority to impose a number of wide-ranging sanctions:

- A monetary penalty (unlimited)
- Suspension from engaging in the Bancassurance business
- Suspension from accessing the credit facilities of the Bank of Tanzania
- Suspension of lending and investment operations
- Suspension of capital expenditure


- Suspension of the privilege to accept new deposits
- Suspension from office of the defaulting director, officer or employee
- Disqualification from any position in any bank or financial institution in Tanzania
- Revocation of banking licence

It is fair to say that whilst the Bancassurance business presents huge opportunities for both banks and insurers alike, both sectors, but particularly the banking sector, must be aware of the obligations and requirements in place when marketing insurance products. ■

Source: Clyde&Co | 1 July 2019


**Total Assets:** US $ 12 billion

**Net Worth:** US $ 5.7 billion
(including US $ 3.5 billion on Fair Value Change Account)

**Global Ranking (2015):**
14th among Global Reinsurers (A M Best)
18th among Global Reinsurers (S & P)

**Ratings:**
**Financial Strength:** A- (Excellent) A M Best Company
**Claims Paying Ability:** "AAA(In)" by CARE

IRDAI Registration No.: 112

GICRE/CAPL/06-16/IQ-001

आपत्काले रक्षिष्यामि

GIC Re

**General Insurance Corporation of India**

Global Reinsurance Solutions

Website: www.gicofindia.in
Contact us at info@gicofindia.com

CIN No.: U67200MH1972GOI016133

# Asian News

## BAHRAIN

### • *Insurance market grows by 6% in 2018*

Insurance premiums in Bahrain grew by 6% to BHD284m ($754m) in 2018, compared to 2017, due to key factors like economic growth, population expansion, as well as increasing life expectancy, a top regulatory official has said.

Central Bank of Bahrain executive director of financial institutions supervision Abdulrahman Al Baker told Gulf Digital News that government investments in infrastructure projects have also provided new underwriting opportunities for further growth of the insurance industry, not just in Bahrain but also in the wider MENA region.

Mr Al Baker said the MENA insurance market will continue to see premium growth of around 5% for the non-life segment and over 7% on the life side.

Looking ahead, he expects further growth in the insurance industry in MENA to be driven by moderate economic growth, despite a slower than expected oil price recovery.

"Sector growth will continue to be supported by large investments in infrastructure and construction projects in the MENA region, further enhancement of regulatory and supervisory standards, as well as the support of governments in making an increasing number of insurance products compulsory.". However, he added that the current global economic uncertainty poses substantial challenges to insurance companies by creating volatility in investment values and returns.

"Public awareness about insurance and its benefits is also another challenge as many fail to recognise insurance as an effective means of wealth protection, savings and security," said Mr Al Baker. ■

Sources: Middle East Insurance Review – 18 June 2019

مصرف البحرين المركزي
Central Bank of Bahrain

Abdulrahman Al Baker

# BAHRAIN

## • *Trust Insurance Management launches new cyber products*

Trust Insurance Management (TIM) has announced the launch of new cyber products. The company has concluded a coverholder agreement to underwrite the cyber insurance products in cooperation with and utilising the experience, expertise and capacity of the Tarian Consortium 9633 (a pool of Lloyd's syndicates led by Beat Syndicate 4242).

TRUST INSURANCE MANAGEMENT W.L.L.


Initially TIM's cyber products are targeted at businesses in the GCC region. Non-property damage losses arising from cyber incidents are covered. More specifically:

Third Party Claims - covers the Insured's liability to third parties from a failure to keep data secure, such as claims for compensation by third parties, investigations, defence costs and fines and penalties from breaching the Privacy Act.

First Party Costs - reimburses the insured for the costs they would incur to respond to a breach, such as IT forensic costs, credit monitoring costs, public relations expenses and cyber extortion costs (including ransom payments to hackers – to the extent insurable by law).

Business Interruption - provides reimbursement for the insured's loss of profits resulting from the breach, as well as any additional necessary expenses it may need to incur to continue business as usual.

In a statement, TIM's CEO Kamal Tabaja said, "Modern business is ever more reliant on technology and connectivity. A breach of data or a service shutdown can have a major risk and financial impact on businesses".

He continued, "As such, we are keen to serve the growing cyber insurance needs in the GCC region, brought about also by the growing awareness of privacy rights, multi-layered legislative approach to data protection laws, increased regional compliance as well as extra-territorial GDPR implications".

TIM is an insurance manager based in Bahrain, regulated by the Central Bank of Bahrain with authorised, issued and paidup capital of BHD100,000 ($266,000). As a subsidiary of Trust Re, TIM has full access to the underwriting expertise and reputation of Trust Re. As a Lloyd's coverholder, TIM is able to offer Lloyd's security and coverage in the more than 200 countries and territories in which Lloyd's operates. ■

Sources: Middle East Insurance Review – 17 June 2019

# FAIR Oil & Energy Insurance Syndicate

## A FAIR Reinsurer with POWER and ENERGY

**Capacity**
Sizeable underwriting capacity for Oil & Energy related business.

**Geographical Scope**
Risks located in Afro-Asian countries and Russia.

**Acceptance Scope**
Business offered by Members, Non-Members, Brokers and all other insurers and reinsurers.

**Underwriting Scope**
The Syndicate underwrites on Facultative basis; Oil & Energy related business including but not limited to:

- Energy: Onshore and Offshore
- Power Plants
- Renewable Energy
- Energy related Constructions
- Nuclear Risks including Radioactive Contamination
- Operators Extra Expenses (Cost of Well Control/Re-drilling Expenses/Seepage and Pollution)
- Business Interruption when written in conjunction with other classes
- Liability when written in conjunction with other classes
- Energy package policies

**A.M Best has assigned the Syndicate the following upgraded ratings:**

Financial Strength Rating (FSR) B+ (Good) with stable outlook.
Issuer Credit Rating (ICR) bbb- with stable outlook

*"The ratings reflect the Syndicate's balance sheet strength, which A.M. Best categorizes as strong, as well as its adequate operating performance, neutral business profile and appropriate enterprise risk management. The rating upgrades reflect the material growth in the syndicate's absolute capital base and the resulting significant improvement in its risk-adjusted capitalization." – A.M Best.*

FAIR Oil & Energy Insurance Syndicate is proud to be the first entity of its kind to be rated by a reputable international rating agency.


*Incorporated in the Kingdom of Bahrain by Law Decree 7/1999*

Managed by
TRUST RE

T: +973 17 517 176 | F: +973 17 533 789
Trust Tower, Building 125, Road 1702, Diplomatic Area 317, Manama
P. O. Box 10844, Manama, Kingdom of Bahrain
foeis@foeis.com | www.foeis.com

# BAHRAIN

## • Afro Asian Assistance Announces New Leadership: Nabil Hajjar, Chairman and Hussain Matooq, General Manager

Nabil Hajjar

Recognising that innovation and strong leadership are key to succeeding in a competitive environment, Afro Asian Assistance today announced leadership changes and outlined its plans for the future.

Known for its expert provision of various services ranging from roadside assistance, travel assistance, Medical Evacuation/Repatriation, Group Personal Accident through its 24/7 Call Centre Services, the Company is mulling plans to diversify its portfolio and to expand its territorial reach. Future considerations also include adapting its business model to become a Third-Party Administrator (TPA).

The appointment of new Board members and a new General Manager reinforces the Company's commitment to continue developing and offering quality services to individuals and companies.

Elected as Chairman of the new Board of Directors is Nabil Hajjar, a seasoned reinsurance expert with a storied career of almost 40 years spanning senior positions in reputable insurance & reinsurance companies in the UAE, USA, Cyprus and Bahrain. Mr. Hajjar held many executive positions within Trust Re since he joined the company in 2000; he is presently Senior Advisor to the Management at Trust Re and Managing Director of the FAIR Oil & Energy Insurance Syndicate.

Commenting on Afro Asian Assistance's plans for the future, Mr. Hajjar said:
"Over the years, the company established itself as a reliable

assistance provider, evident by the sound reputation and the large number of clients in various countries. With the new Board of Directors and new management team, we will work on reinforcing the company's strengths, reform our vision, mission and values, maintain sound corporate governance and build new strategies to meet our objectives".

He continued, "Amongst other important strategies, we will capitalise on the present achievements, focus on human capital and develop team skills in order to further enhance the quality of our service, introduce new products, and expand our geographical scope of service. In brief, we aim at being The Assistance Team that Cares."

Kamal Tabaja (Deputy Chairman of the BoD), Eslam Elbahy (General Secretary & Member), Ali Mohsen (Member) and Mohsin Altaf (Member) complete the 5-person Board.

Collectively, the BoD sets the overall strategic direction, approves business plans and monitors the overall performance of the business against approved strategic plans and within a framework of sound corporate governance.

The Board of Directors appointed Hussain Matooq as General Manager, effective 1 July 2019. Mr. Matooq brings with him over 20 years' experience working in the reinsurance industry. Prior to his appointment at Afro Asian Assistance, he was Head of Operational Services at Trust Re with overall responsibility for Claims, Technical Accounts, Risk Engineering and Quality Process Improvement departments. His key strengths include enhancing business processes and procedures as well as strategic projects.

Mr. Matooq remarked, "As a team, we are motivated by the prospects of evolving from a primarily Afro Asian assistance services company to one with a wider global reach, offering innovative products and optimising the use of technology at all times".

Working closely with Mr. Matooq to lead the dedicated Afro Asian Assistance team is Ahmed Nasralla, Deputy General Manager and Head of Business Development since 2013. With over 20 years of experience and well known in the market, Mr. Nasralla highlighted some of the key reasons behind the Company's success to date.

He said, "We are proud to have developed a healthy relationship with clients; it is a relationship of trust which we look forward to building on further under the auspices of our new Board and leadership". Ahmed further cited the Company's speed in turnaround time as a key factor in maintaining excellent relationships with its business partners. ■

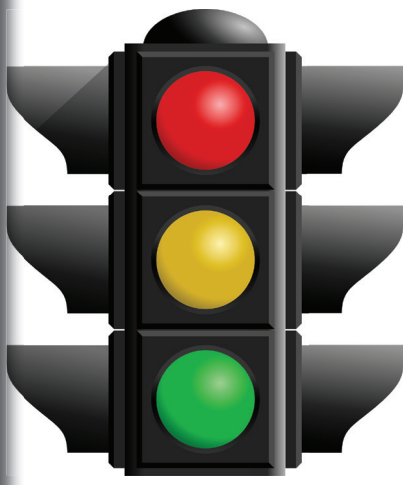
Hussain Matooq

Ahmed Nasralla

# CHINA

## • *Optimism That China Insurance Intermediary Licence Approvals Will Re-Start*

Article by Michael Cripps and Xiaolin Lin (Clyde & Co)



In early June 2019, the China Banking & Insurance Regulatory Commission ("CBIRC") circulated (intra-industry only) a draft paper 'Discussion Draft Regulations re the Administration of Insurance Intermediaries Approval & Registration' ("Draft Regulations"). The Draft Regulations aim to integrate and unify the existing regulatory landscape governing market entry and access in the insurance intermediated sector ("Intermediated Sector"). The Draft Regulations aim to tighten and standardise criteria and requirements for insurance intermediaries in China ("Intermediary").

In some respects, the Draft Regulations actually raise the bar for those looking for entry into the Intermediated Sector. Any applicant looking to enter the Intermediated Sector must demonstrate its thorough planning, understanding and market positioning of its Intermediary in the Intermediated Sector, assuming approval is granted. Further, applicants must understand that their Intermediary will be subject to strict regulatorily-mandated risk assessment and risk testing, in order to identify whether there would ever be any risk of the approved Intermediary conducting any aspect of its business in an unlawful manner. Applicants must clearly demonstrate that an approved Intermediary will be able to operate independently of its parent shareholder(s) with respect to the Intermediary's personnel, business, assets and financing.

The Draft Regulations crystallise and finesse 'fit-and-proper' criteria for proposed appointees to senior management roles within Intermediaries. Interestingly, some of these criteria include (i) no conduct, within the prior five years, of 'public morality outrage'; (ii) no conduct, within the prior three years, of any breach of professional ethics, failure of integrity, or severe failure in work, where such breach or failure caused material harm or adverse impact; and, (iii) within the prior two years, neither direction of, nor active involvement in, any failure to co-operate in a regulatory investigation of an entity in which that proposed appointee was then employed.

Public commentary has indicated that CBIRC has approved no new Intermediary licences since August 2018. Assuming the Draft Regulations become at some stage formally promulgated into law, then the expectation is that CBIRC would then resume approving Intermediary licence applications. ■

24 June 2019

# INDIA

## • *Indian government considers plan to merge all four state-owned non-life carriers*

By Adrian Ladbury on June 26, 2019

Leading Indian newspapers report that the Indian government is planning to form a single state-owned mega non-life insurer through the merger of all four state-run insurers: Oriental, National, United India and New India.

The Indian government announced plans to merge Oriental, National and United India in its 2018 budget. The latest news is that the government is now looking into the idea of New India taking over the other three once merged together.

The Economic Times reported that a government official said that if Oriental, National and United were to be merged into one entity as previously discussed, the merged entity would simply compete against New India and the two sides would undercut each other.

The newspaper reported that the government has decided that this would not make sense and is therefore considering the merger of the first three insurers and then having the listed New India acquire the merged entity.

The newspaper also reported that the government is likely to announce an injection of INR40bn ($573m) into the three state-owned and non-listed companies to boost their capital.

According to The Economic Times, latest data from the Indian insurance supervisor, the IRDAI, shows that New India has a market share of 16.8% in terms of gross direct premium. If combined with the other three carriers, its market share would rise to about 25%.

If two other state-owned non-life insurers – Agriculture Insurance Company and Export Guarantee Corporation of India – were added, then that market share would lift to a massive 45.35%, according to the IRDAI.

Business Standard newspaper subsequently reported that most employees of the four state-owned non-life insurers are in favour of the proposed merger.

The newspaper reported that employee unions of the insurers say that a merger will end competition among the companies and help them reclaim market leadership.

A E Shantakumar, president of the United India Insurance Officers Union, told Business Standard: "The merger of all the companies would be a better idea than the merger of three, as it will become a strong entity and after capital infusion, will be able to underwrite big businesses." ■

Commercial Risk 26 June 2019

# IRAQ

### • *Islamic banks establish takaful company*

The Central Bank of Iraq has established a takaful company for Islamic banks in cooperation with the Insurance Bureau.

The takaful company has a capital of IQD15bn ($12.7m) with the participation of all Islamic banks in the country, reported the daily newspaper Azzaman.

"The company's takaful controls have been formulated in accordance with the standards of the Islamic Financial Services Board (IFSB) and the Accounting and Auditing Organization for Islamic Financial Institutions," the bank said in a statement.

The establishment of the Islamic insurer is an important move in the comprehensive strategic plan of the Bank to develop the Islamic banking industry. ■

Sources: Middle East Insurance Review – 25 June 2019

# SAUDI ARABIA

### • *Saudi insurers face solvability problems*

Multiple Saudi insurance companies are having hard times with their Shareholders' equity. At 31 December 2018, 12 over 31 companies operating in the market recorded shareholders' equity lower than their capital.

Such an abnormal and risky situation can be traced back to accumulated losses over the years, pushing the insurers to draw from their Shareholders' Equity. Although having been authorized to reduce their capital to improve the results, the insurers' situation remains critical.

In order to consolidate the market, the authorities plan to increase the minimum capital of insurers, from 100 million SAR (26.6 million USD) to 500 million SAR (133.2 million USD). If such a strategy were to be applied, only Bupa Arabia and Tawuniya would be in accordance with the new threshold. To continue to operate, the other companies would have to review the situation with their shareholders.

## Saudi insurers' capital and equity positions in 2018 :

### Saudi insurers whose shareholder's equity to capital ratio is equal to or above 100%

| | Insurer | Capital | | Shareholders' equity | | Shareholder's equity to capital ratio |
|---|---|---|---|---|---|---|
| | | IN SAR | In USD | In SAR | In USD | |
| 1 | Bupa Arabia | 1200 | 319 | 2574 | 685 | 215 |
| 2 | Al-Rajhi | 400 | 106 | 768 | 204 | 192 |
| 3 | Buruj | 250 | 67 | 454 | 121 | 181 |
| 4 | Trade Union | 275 | 73 | 432 | 115 | 157 |
| 5 | Walaa | 440 | 117 | 671 | 179 | 152 |
| 6 | Tawuniya | 1250 | 333 | 1899 | 506 | 152 |
| 7 | Chubb | 200 | 53 | 293 | 78 | 147 |
| 8 | Arabian Shield | 300 | 80 | 428 | 114 | 143 |
| 9 | Al Ahli | 167 | 44 | 235 | 63 | 141 |
| 10 | AXA | 200 | 53 | 268 | 71 | 134 |
| 11 | Allianz | 450 | 120 | 590 | 157 | 131 |
| 12 | Watanya | 200 | 53 | 240 | 64 | 120 |
| 13 | Jazira | 350 | 93 | 398 | 106 | 114 |
| 14 | Gulf Union | 150 | 40 | 167 | 44 | 112 |
| 15 | SAQR | 400 | 106 | 442 | 118 | 110 |
| 16 | SAICO | 300 | 80 | 321 | 85 | 107 |
| 17 | Salama | 250 | 67 | 264 | 70 | 106 |
| 18 | SABB | 340 | 91 | 346 | 92 | 102 |
| 19 | Solidarity | 250 | 67 | 251 | 67 | 100 |

### Saudi insurers whose shareholder's equity to capital ratio is below 100%

| | Insurer | Capital | | Shareholders' equity | | Shareholder's equity to capital ratio |
|---|---|---|---|---|---|---|
| | | IN SAR | In USD | In SAR | In USD | |
| 1 | Alamiya | 400 | 106 | 387 | 103 | 97 |
| 2 | Arabia | 265 | 71 | 251 | 67 | 95 |
| 3 | UCA | 400 | 106 | 361 | 96 | 90 |
| 4 | Malath | 500 | 133 | 450 | 120 | 90 |
| 5 | MetLife | 180 | 48 | 154 | 41 | 85 |
| 6 | MedGulf | 800 | 213 | 672 | 179 | 84 |
| 7 | Tokio Marine | 300 | 80 | 246 | 65 | 82 |
| 8 | Gulf General | 200 | 53 | 159 | 42 | 80 |
| 9 | Al Ahlia | 160 | 43 | 123 | 33 | 77 |
| 10 | ACIG | 200 | 53 | 138 | 37 | 69 |
| 11 | Amana | 140 | 37 | 96 | 26 | 68 |
| 12 | Enaya | 100 | 27 | 56 | 15 | 56 |

# Thailand

## • Compulsory health insurance for foreigners over 50 years visiting Thailand

People aged 50 years and above wishing to have a long stay in Thailand will have to comply with the requirements of the new immigration regulations. The latter requires the underwriting of a health insurance cover for any long-stay visa application.

The cover must be of 40 000 THB (1 264 USD) for ambulatory treatment and of 400 000 THB (12 600 USD) maximum for hospital treatment.

The measure introduced aims at ease the financial burden of public health care bodies, overwhelmed by the management of foreign patients who do not have any sufficient resources.

The government has established a first list of countries whose citizens will have to present an insurance policy. Insurance policies underwritten outside the country are accepted. ■

Source: Atlas Magazine – 20 May 2019


# TURKEY

## • Turkey to create SDDK - the new independent Insurance Regulation and Supervision Authority

Turkish authorities are ready to set up SDDK - the new independent Insurance Regulation and Supervision Authority, according to the Minister of Treasury and Finance, Berat ALBAYRAK quoted by Middle East Insurance Review.

The SDDK is part of Turkey's "New Economy Programme Structural Transformation Steps 2019" announced last month, that promises structural reforms for the financial sector. Currently, the Treasury supervises and regulates the insurance industry, an industry where it operates more than 60 companies with foreign investors commanding around 70% of the market.

Can Akin CAGLAR, Turkey Insurance Association President (TSB) said that the establishment of the SDDK would expand the insurance industry because "the legislative arrangements will be released much more quickly, and the market will be more driven in anticipation of expectations and needs" (Middle East Insurance Review). ■

Sources: XPRIMM – 5 June 2019

# KAZAKHSTAN:

## INSURANCE MARKET OVERVIEW

by Hussein Elsayed
*Misr Insurance Company*


## ( I ) SOCIO-ECONOMIC DATA

**Land Area**
2,699,700 sq km

**Capital**
Nur-sultan
(Previously: Astana)

**Population**
18.19 million (2017)*
World ranking: 63/191

**Median Age**
29.3 (2015)
World ranking: 96/201

**Language**
Kazakh (Official)
Russian (Official)

**Religion**
Muslims (70.4%)
Orthodox (20.2%)
Unaffiliated (4.2%)

**Political System**
Unitary republic

**Currency**
(Period Average)
Kazakhstani Tenge
326.00 per US$ (2017)

**Economic Structure**
(in terms of GDP composition, 2017)
Agriculture (4.00%)
Industry (32.00%)
Services (57.40%)

| | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|
| Population (million) | 17.2 | 17.4 | 17.7 | 17.9 | 18.2 |
| GDP per capita (USD) | 13,591 | 12,481 | 6,793 | 7,852 | 8,773 |
| GDP per capita (EUR) | 9,863 | 10,314 | 6,253 | 7,445 | 7,306 |
| GDP (USD bn) | 233 | 217 | 120 | 141 | 160 |
| GDP (EUR bn) | 169 | 180 | 110 | 133 | 133 |
| Economic Growth (GDP, annual variation in %) | 6.0 | 4.2 | 1.2 | 1.1 | 4.1 |
| Consumption (annual variation in %) | 10.6 | 1.1 | 1.8 | 1.2 | 1.2 |
| Investment (annual variation in %) | 5.5 | 4.4 | 4.2 | 3.0 | 4.0 |
| Industrial Production (annual variation in %) | 2.3 | 0.2 | -1.6 | -1.2 | 7.2 |
| Unemployment Rate | 5.2 | 5.0 | 5.1 | 4.9 | 4.9 |
| Fiscal Balance (% of GDP) | -1.9 | -2.7 | -2.2 | -1.6 | -2.7 |
| Public Debt (% of GDP) | 12.3 | 14.3 | 22.1 | 24.4 | 25.5 |
| Money (annual variation of M2 in %) | 1.5 | -8.2 | 8.0 | 46.2 | 7.5 |
| Inflation Rate (CPI, annual variation in %, eop) | 4.8 | 7.4 | 13.6 | 8.5 | 7.1 |
| Inflation Rate (CPI, annual variation in %) | 5.8 | 6.7 | 6.6 | 14.7 | 7.4 |
| Policy Interest Rate (%) | 6.50 | 6.50 | 16.00 | 12.00 | 10.25 |
| Exchange Rate (vs USD) | 154.4 | 182.9 | 340.6 | 333.7 | 332.8 |
| Exchange Rate (vs USD, aop) | 152.2 | 179.4 | 223.3 | 342.0 | 326.3 |
| Exchange Rate (vs EUR) | 212.2 | 221.2 | 369.9 | 350.9 | 399.3 |
| Exchange Rate (vs EUR, aop) | 202.2 | 238.3 | 247.5 | 378.6 | 369.0 |
| Current Account (% of GDP) | 0.8 | 2.8 | -5.0 | -5.8 | -3.2 |
| Current Account Balance (USD bn) | 2.0 | 6.1 | -6.0 | -8.1 | -5.1 |
| Trade Balance (USD billion) | 36.0 | 36.6 | 11.6 | 9.3 | 16.7 |
| Exports (USD billion) | 85.1 | 79.1 | 44.8 | 35.5 | 47.3 |
| Imports (USD billion) | 49.2 | 42.5 | 33.2 | 26.2 | 30.6 |
| Exports (annual variation in %) | -1.6 | -7.1 | -43.3 | -20.8 | 33.3 |
| Imports (annual variation in %) | 5.4 | -13.7 | -21.8 | -21.0 | 16.5 |
| International Reserves (USD) | 24.7 | 29.2 | 27.9 | 29.7 | 31.0 |
| External Debt (% of GDP) | 64.3 | 72.3 | 127 | 116 | 105 |

Kazakhstan has a land area equal to that of Western Europe but one of the lowest population densities globally. Strategically, it links the large and fast-growing markets of China and South Asia and those of Russia and Western Europe by road, rail, and a port on the Caspian Sea.

Kazakhstan has transitioned from lower-middle-income to upper-middle income status in less than two decades. The country moved to the upper-middle-income group in 2006. Since 2002, GDP per capita has risen sixfold and poverty incidence has fallen sharply, showing significant progress in country performance in the World Bank's indicator of shared prosperity.

Kazakhstan's challenging external environment caused a broad-based economic slowdown in 2014 and put upward pressure on inflation. Progress on poverty reduction was largely stagnant in 2014 and 2015, reflecting slow growth and weak labor market outcomes. In 2017, more favorable terms of trade and increased oil production supported an economic recovery and an improvement in poverty indicators.

Ongoing structural and institutional reforms aim to reduce the role of the state in the economy and facilitate the development of a vibrant, modern, and innovative tradable non-oil sector.

Real GDP expanded by 4.1 percent in 2018 on the back of stronger exports and recovering domestic demand. Net exports continued to contribute substantially to GDP due to stronger-than-expected production from the Kashagan oil field, though the impetus appears to be diminishing as production flattens. Private consumption rose by an estimated 4.5 percent, benefiting from rising incomes and moderating inflation.

GDP growth is projected to decelerate slightly in 2019–20 and flatten thereafter. The outlook reflects slow productivity growth and the underlying structural weaknesses of the economy, including market dominance by state-owned enterprises, the unequal regulatory treatment of enterprises, and the low level of competition.

Boosted by rising real wages, consumer spending will continue to drive economic activity, though to a lesser extent than in previous years. Government initiatives to provide subsidized mortgage and car purchase loans will also support private consumption. The non-oil fiscal deficit is expected to decline further in line with the Government's medium-term fiscal consolidation strategy.

The NBK is expected to raise the key policy rate to counter inflationary pressures from real wage growth, thereby keeping inflation within the 2019 target range.

The tax cut for low income earners and the 50 percent increase in the minimum wage in January 2019, along with a tight labor market, are expected to stabilize the poverty rate at around 5 percent by 2021.

THE WORLD BANK

*Source:*
*The World Bank – April 2019*

## Risks

### Sovereign Credit Ratings

*Sources: Moody's, Standard & Poor's, Fitch Ratings*

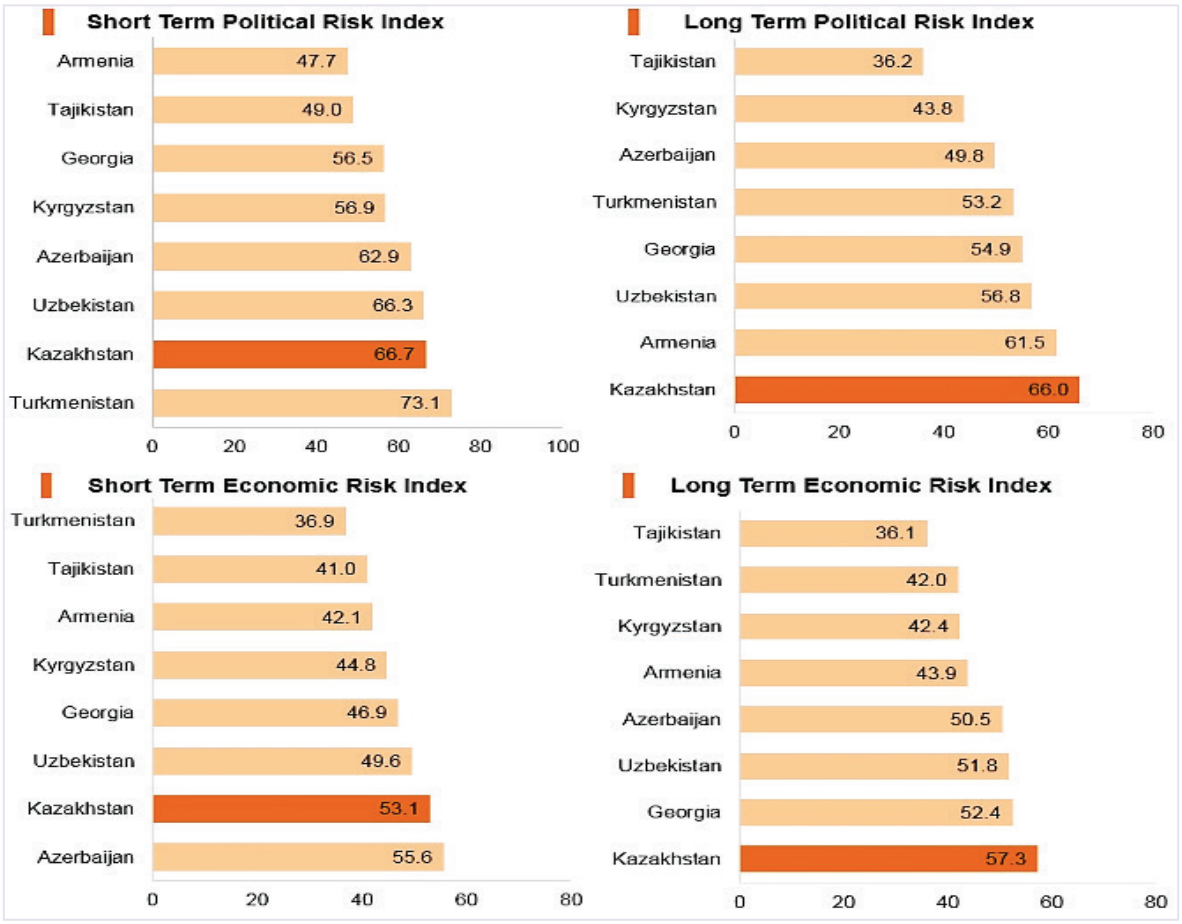
| | Rating (Outlook) | Rating Date |
|---|---|---|
| **Moody's** | Baa3 (Stable) | 26/07/2017 |
| **Standard & Poor's** | BBB- (Stable) | 17/02/2016 |
| **Fitch Ratings** | BBB (Stable) | 28/09/2018 |

### Competitiveness and Efficiency Indicators

*Sources: World Bank, IMD, Transparency International*

| | World Ranking | | |
|---|---|---|---|
| | **2017** | **2018** | **2019** |
| **Ease of Doing Business Index** | 35/189 | 36/190 | 28/190 |
| **Ease of Paying Taxes Index** | 60/189 | 50/190 | 56/190 |
| **Logistics Performance Index** | N/A | 71/160 | N/A |
| **Corruption Perception Index** | 122/180 | 124/180 | N/A |
| **IMD World Competitiveness** | 32/63 | 38/63 | N/A |

## Political and Economic Risk Indices




100 = Lowest risk, 0 = Highest risk

*Source: Fitch Solutions February 19, 2019*

### Operational Risk Index

100 = Lowest risk, 0 = Highest risk

| Country | Operational Risk Index | Labour Market Risk Index | Trade and Investment Risk Index | Logistics Risk Index | Crime and Security Risk Index |
|---|---|---|---|---|---|
| Georgia | 61.9 | 64.7 | 70.9 | 54.9 | 57.1 |
| Azerbaijan | 58.8 | 60.3 | 62.4 | 59.5 | 52.8 |
| Kazakhstan | 58.5 | 71.6 | 58.9 | 54.1 | 49.3 |
| Armenia | 55.5 | 56.1 | 58.5 | 49.9 | 57.6 |
| Uzbekistan | 42.3 | 51.2 | 53.1 | 34.7 | 32.5 |
| Tajikistan | 42.3 | 52.8 | 38.9 | 38.8 | 40.1 |
| Kyrgyzstan | 42.3 | 49.2 | 44.7 | 38.0 | 33.5 |
| Turkmenistan | 38.1 | 33.8 | 39.4 | 43.1 | 36.1 |
| Caucasus and Central Asia Average | 50.0 | 54.9 | 53.4 | 46.6 | 44.9 |
| Emerging Markets Averages | 46.7 | 48.0 | 45.5 | 47.4 | 46.0 |
| Global Markets Averages | 49.6 | 49.7 | 49.9 | 49.0 | 49.8 |

*Source: Fitch Solutions February 19, 2019*

## Natural Hazards

Earthquakes in the south | Mudslides around Almaty

# (II) KAZAKH INSURANCE MARKET

## History of Insurance Market and its Evolution

- **1921** Insurance was first introduced with the establishment of the Soviet state insurance company, Gosstrakh
- **1940** Agricultural insurance was made compulsory for collective farms.
- **1976** Agricultural insurance for state farms on a compulsory basis was introduced.
- **1989** A law on co-operatives allowed the first co-operative insurers to be set up. They were later transformed into joint stock companies. The insurance of state property was permitted.
- **1991** Private sector insurance companies grew rapidly. Domestic cargo insurance was reintroduced. Gosstrakh USSR broke up into independent national companies.
- **1992** The first law on insurance came into force in September (Law No 1510-XII dated 3 July 1992 On Insurance). Compulsory motor third party liability for commercially owned vehicles was introduced.
- **1993** Decree 2087 required foreign investors to insure their risks with local insurers, banned foreign insurers from acting in Kazakhstan in any form (including joint ventures) and removed tax deductibility from non-compulsory insurance premiums.
- **1995** A new insurance law was issued. Foreign ownership of joint ventures up to 50% was permitted and capital requirements were increased.
- **1997** Motor third party liability insurance was made compulsory from 1 January.
- **1999** Various regulations covering all aspects of establishing a company, constitution of capital, establishment of technical reserves etc were issued by the National Bank.
- **2001** Revised insurance legislation and regulations were issued.
- **2002** All state-owned insurers were privatised, with the exception of the wholly owned export guarantee company. In the same time insurance premiums were no longer regarded as an allowable expense for tax purposes.
- **2005** Workers' accident insurance was established as a compulsory class from 1 July. It was made the exclusive province of life insurance companies in 2012.
- State Annuity Company was established to offer annuities in respect of personal injury cases (workers' accident only).
- **2006** New regulations were introduced regarding the cession of reinsurance to foreign companies.
- Compulsory environmental impairment insurance was introduced (known locally as "dangerous facilities" insurance).
- **2009** In February the regulator endorsed the move to take into partial state ownership four of the leading commercial banks, all of which have insurance subsidiaries.
- **2011** Regulation of the insurance market was passed to the National Bank of Kazakhstan.
- **2015** Kazakhstan's accession to the World Trade Organization on 30 November provides foreign insurance organisations greater access to the Kazakhstan insurance market.
- On 2 July **2018** a significant package of amendments to insurance related laws was adopted aimed at the improvement of transparency and governance and the introduction of additional consumer protection measures. From 16 December non-admitted insurance was permitted for marine, commercial aviation, space and transportation risks.

# Regulatory Framework

## ➢ INSURANCE LAW:

- ***Chapter 40, Articles 803 to 845 of the special part of the Civil Code*** of the Republic of Kazakhstan deals with insurance and describes the conclusion of insurance contracts, their contents and termination conditions, as well as concepts such as the duty of disclosure, change in level of risk, subrogation etc.
  Mutual insurance and Islamic insurance are also referenced in the Civil Code.
- ***Law No 126-II* dated 18 December 2000 *On Insurance Activity***

## ➢ SUPERVISORY AUTHORITY:

The functions of regulating the insurance market are carried out by **the Department of Insurance Supervision of the National Bank of Kazakhstan** (the regulator). This department is consists of three sub-departments covering methodology and draft legislation, off-site supervision, and on-site supervision (also a sub-department of the audit department for all financial activities).

NATIONAL BANK OF KAZAKHSTAN
OFFICIAL INTERNET-RESOURCE

https://nationalbank.kz/

Kazakhstan has had one of the more advanced and effective supervisory bodies in the Commonwealth of Independent States (CIS), focused mainly upon ensuring consumer protection through solvency, but also maximizing the use of the capacity of the local insurers whilst still ensuring reliable reinsurance protection but controlling export of premium to dubious offshore zones. Most insurers are inspected regularly, as are the operations of the representative offices of international brokers.

## ➢ COMPULSORY INSURANCES:

- Fund for road, rail, sea and air transport passengers - State Social Insurance Scheme.
- Motor third party liability.
- Carriers' liability insurance for damage caused to the life, health and property of passengers on public transport by sea, air, rail and road.
- Crop insurance.
- Professional indemnity for notaries.
- Professional indemnity for auditors.
- Compulsory travel insurance of (outbound) tourists organized through travel agents and/or tour operators.
- Workers' accident insurance.
- Ecological insurance - environmental liability for businesses carrying on environmentally hazardous activities.
- Third party liability for the owners of dangerous facilities.
- Ship owners' liability for marine oil pollution (financial guarantee or insurance).
- Third party liability of sponsors of clinical trials against damages to the life and health of participants in clinical trials (licensing requirement).

## ➢ STATUTORY TARIFFS:

Statutory premium tariffs are set for the main compulsory classes of insurance which are subject to their own separate laws.
Tariffs are not set for non-compulsory classes: insurers are free to charge what they deem to be commercial rates for the business.

## ➢ POOLS:

There are no pools active in the Kazakh market.

## ➢ CAPITAL REQUIREMENT

*The minimum authorized capital for a newly created insurance/reinsurance organization must equal:*

- when seeking a licence in the 'general insurance' sector – 430 (four hundred and thirty) million tenge;
- when seeking a licence in the 'life insurance' sector – 670 (six hundred and seventy) million tenge;
- when seeking a licence in the 'general insurance' sector and a reinsurance licence – 450 (four hundred and fifty) million tenge;
- when seeking a licence in the 'life insurance' sector and reinsurance licence – 690 (six hundred and ninety) million tenge; and
- when seeking a reinsurance licence, with reinsurance being the only line of business – 530 (five hundred and thirty) million tenge.

The timeframe for granting permission is within three months of the date when the applicant filed the last documents requested by the authorized body, as per the law on insurance, but no later than six months from the date of receiving an application.

## ➢ FOREIGN OWNERSHIP & FDI RESTRICTIONS

There are no restrictions on foreign ownership of an insurance/reinsurance company in Kazakhstan, except that a prospective foreign owner must have a financial strength rating from an officially recognized rating agency which meets the minimum requirements of the regulator.

## ➢ SUBSIDIARY/BRANCH

Branches of foreign insurance/reinsurance companies are not yet permitted to operate in Kazakhstan until the end of the WTO accession transition period (16 December 2020); A non-resident insurance/reinsurance organization wishing to open a branch may, at the Kazakhstan government's option, be required to evidence total assets of not less than USD 5bn and at least 10 years of experience in the sector and classes in which it applies to operate.

The Monument of Independence, Republic Square.

## ➢ BROKERS:

- Insurance brokers are required to be registered and are subject to licensing by the regulator. At present, the role of brokers is mainly limited to servicing the larger commercial risks including employee benefits programmes, but their role is expanding as the need for professional advice is increasingly recognized.
- Resolution No 270 dated 29 October 2018 came into effect on 1 January 2019 and established increased minimum authorized capital for brokers of 20,000 multiples of the monthly calculation index (equivalent to USD 154,640 based on a monthly calculation index set at KZT 2,525 (USD 7.73) for 2019) for insurance broker activities and 100,000 multiples (equivalent to USD 773,201) for reinsurance broking activities respectively. Existing licence holders were granted until 1 July 2021 to comply.

## ➢ NON-ADMITTED

- There is no requirement for overseas insurers/reinsurers to be registered, licensed, supervised or to put up deposits. A foreign reinsurer is not required to have a specific rating as such but ceding insurers/reinsurers may have to increase their solvency capital or guarantee fund depending on the rating, so at least "A-" is desirable ("BBB-" for countries of the Eurasian Economic Union which would include Russia and Belarus).
- Insurers can take credit for accounting/solvency margin purposes for reinsurance placed abroad, bearing in mind the above scale.


## ➢ REINSURANCE

- There are no local reinsurance companies in Kazakhstan and there are no compulsory reinsurance cessions or insurance pools currently in effect in Kazakhstan.
- Several of the larger local direct writing companies do accept some inwards reinsurance through facultative placements.
- From 15 July 2018 new restrictions apply relating to the use of foreign (re)insurance brokers when placing reinsurance overseas. A local insurer can only cede reinsurance overseas via a foreign broker if that

## ➢ TAXES

- The government of Kazakhstan imposes corporate income tax at 20%; capital gains are taxed at 20% and exempts dividends from taxation.

## ➢ ALTERNATIVE RISK TRANSFER

- Alternative risk transfer (ART) is unknown.

# Insurance Market Performance and Statistics

*As of January 1, 2019, the Kazakh market was represented by the following:*

- 28 active insurance companies (6 of which were life companies and 22 of which are non-life).
- 14 registered insurance brokers.
- 56 registered actuaries.

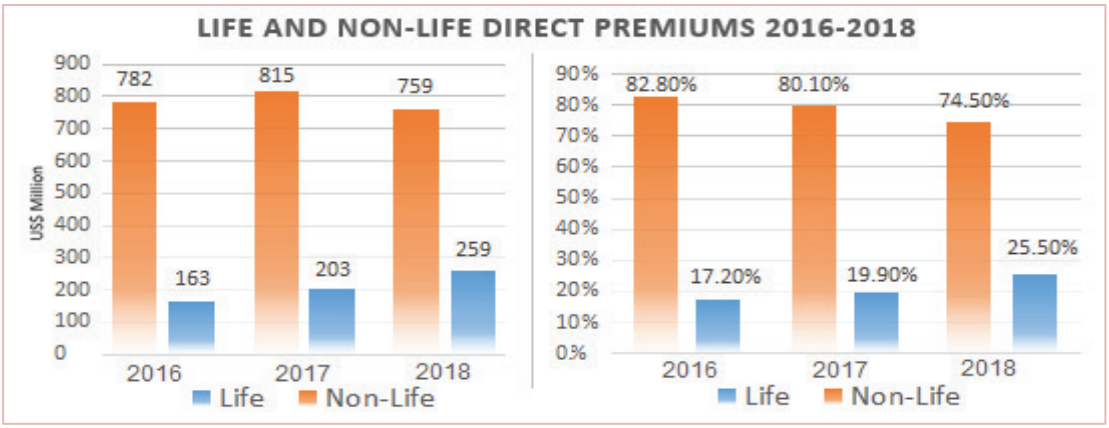
| Total Premiums | 2016 | 2017 | 2018 |
|---|---|---|---|
| Total Direct Premiums (US$ m) | 945 | 1018 | 1018 |
| Real Premium Growth (%) inflation-adjusted | 7.1% | -4.4% | -0.4% |
| Penetration (% of GDP) | 0.7% | 0.7% | 0.63% |
| Density (per capita in US$) | 53 | 62 | 55 |
| Share of World Total Premiums (%) | 0.02% | 0.02% | 0.02% |
| Global Ranking (WP) | 76 | 73 | 77 |
| Global Ranking (Penetration ) | 84 | 83 | 84 |
| Global Ranking (Density ) | 75 | 75 | 78 |

| Life Premiums | 2016 | 2017 | 2018 |
|---|---|---|---|
| Life Direct Premiums (US$ m) | 163 | 203 | 259 |
| Share of Country Total Premiums (%) | 17.2% | 19.9% | 25.5% |
| Real Premium Growth (%) inflation-adjusted | -16.6% | 10.5% | 27.1% |
| Life Penetration (% of GDP) | 0.12% | 0.12% | 0.16% |
| Life Density (per capita in US$) | 9.1 | 10 | 14 |
| Share of World Life Premiums (%) | 0.01% | 0.01% | 0.01% |
| Global Ranking | 78 | 74 | 72 |

| Non-Life Premiums * | 2016 | 2017 | 2018 |
|---|---|---|---|
| Non-Life Direct Premiums (US$ m) | 782 | 815 | 759 |
| Share of Country Total Premiums (%) | 82.8% | 80.1% | 74.5% |
| Real Premium Growth (%) inflation-adjusted | 12.1% | -7.5% | -7.3% |
| Non-Life Penetration (% of GDP) | 0.56% | 0.67% | 0.47% |
| Non-Life Density (per capita in US$) | 43.9 | 50 | 41 |
| Share of World Non-Life Premiums (%) | 0.04% | 0.04% | 0.03% |
| Global Ranking | 72 | 70 | 74 |

* *Include PA&H Insurance*

*Source: Swissre Sigma Explorer*

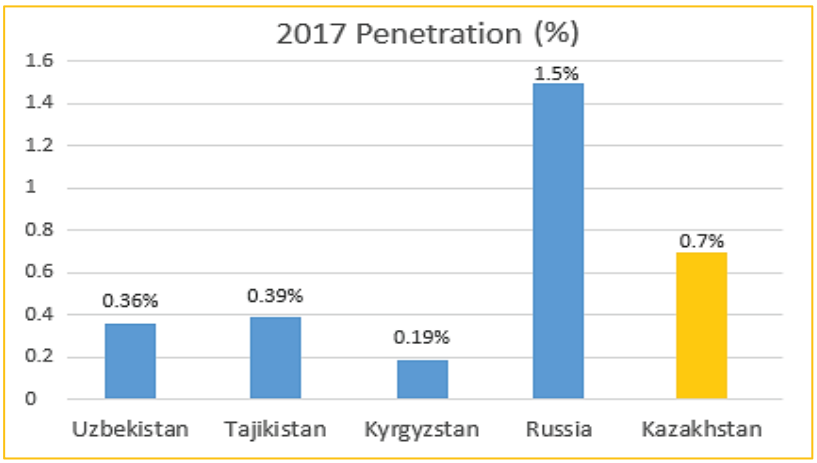


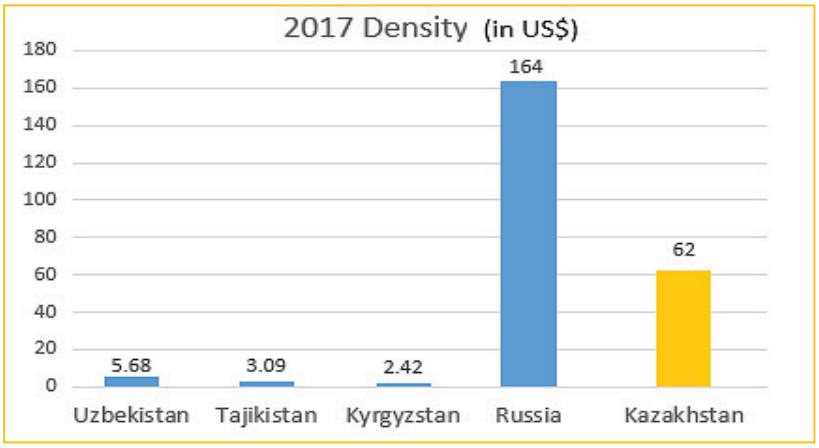
According to Sigma, the research publication of Swiss Re, the Kazakh insurance market ranked 77th among world markets in 2018, ahead of Cyprus, Allinsurance.kz reported with reference to Express-k.kz.

As Sigma's analysis shows, the Kazakh non-life sector was ahead of Serbia, Pakistan and Tunisia last year, but with a large margin from Russia and Ukraine.

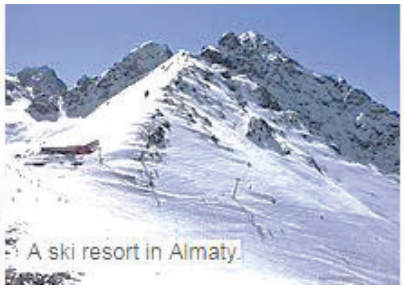
Among the key analytical criteria, Sigma noted a decrease of insurance GWP per capita in Kazakhstan, to USD 55 in 2018 vs USD 61 in 2017. In Russia, this figure in 2018 increased by 8% to USD 164, and in western developed countries it ranged from USD 1,000 to USD 7,000, Allinsurance.kz reports.

Market premium as a percentage of GDP and expenditure on a per capita basis expressed in US$ for the year 2017; comparisons are made with Russia, Kyrgyzstan, Tajikistan and Uzbekistan.



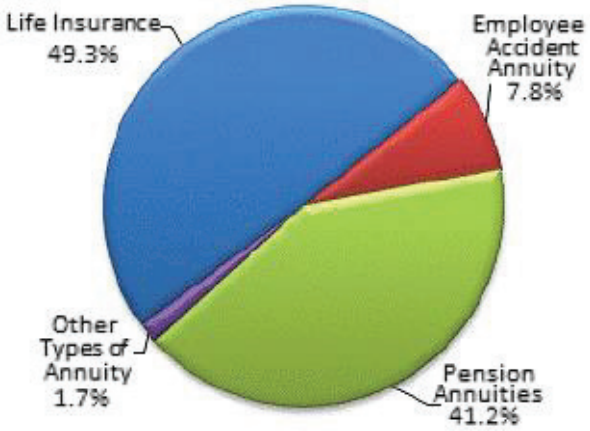





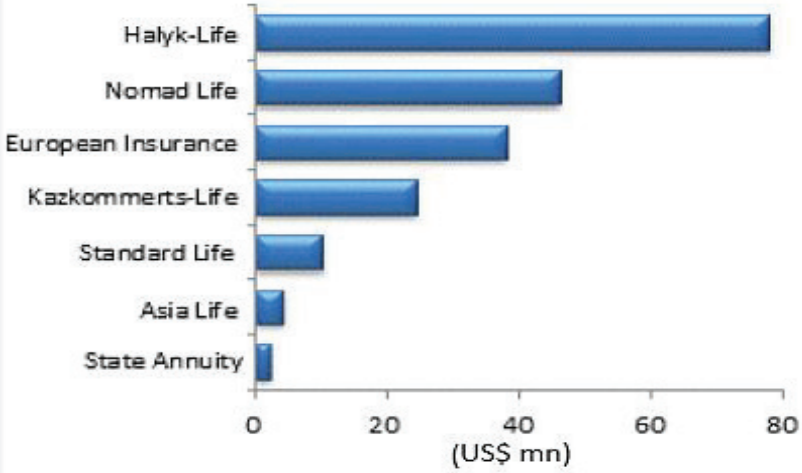



## Life Business

### Breakdown of Life by Line of Business 2017




### Leading Life insurance companies in 2017




### Life Market Concentration (%)

| | 2015 | 2016 | 2017 |
|---|---|---|---|
| Top 3 companies | 67.84 | 69.53 | 79.78 |
| Top 5 companies | 89.32 | 94.72 | 96.81 |

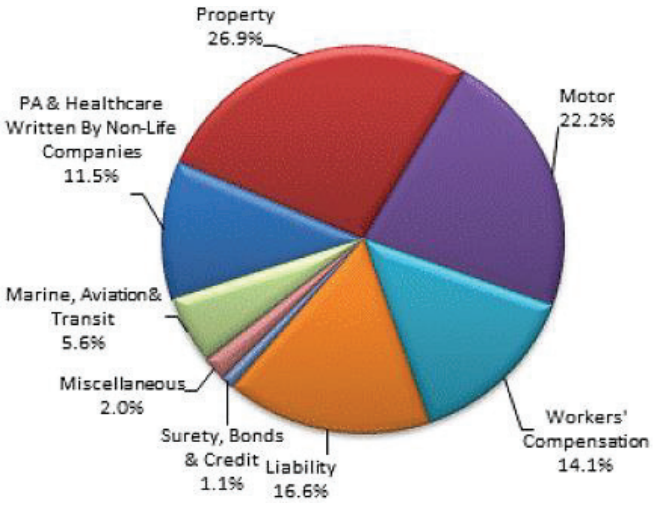
### Life Distribution Channels (%)

| | 2016 | 2017 | 2018 |
|---|---|---|---|
| Direct | 50 | 45 | 40 |
| Broker | 2 | 2 | 1 |
| Agent | 13 | 12 | 10 |
| Bancassurance | 35 | 41 | 49 |

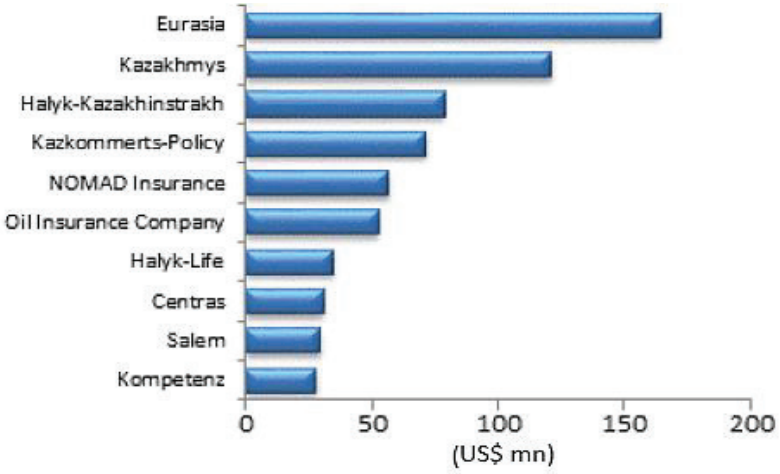
The mountainous region of the Tian Shan in south-eastern Kazakhstan

## Non-Life Business

## Breakdown of Non-Life by Line of Business 2017




## Leading Non-Life insurance companies in 2017




### Non-Life Market Concentration (%)

| | 2015 | 2016 | 2017 |
|---|---|---|---|
| Top 5 companies | 46.73 | 52.48 | 52.76 |
| Top 10 companies | 68.42 | 71.31 | 71.48 |

### Non-Life Distribution Channels (%)

| | 2016 | 2017 | 2018 |
|---|---|---|---|
| Direct | 30 | 32 | 35 |
| Broker | 15 | 15 | 15 |
| Agent | 35 | 33 | 30 |
| Bancassurance | 20 | 20 | 20 |

## Non-Life Loss Ratios 2015-2017 (%)

| | 2015 | 2016 | 2017 |
|---|---|---|---|
| Property | 23.12% | 28.33% | 14.32% |
| Motor | 42.82% | 44.97% | 43.28% |
| Construction & Engineering | NA | NA | NA |
| Workers' Compensation | 26.25% | 15.47% | 16.32% |
| Liability | 3.64% | 7.25% | 2.49% |
| Surety, Bonds & Credit | 0.15% | 22.33% | 36.56% |
| Miscellaneous | 9.28% | 2.20% | 16.43% |
| Marine, Aviation & Transit | 15.12% | 18.27% | 24.09% |

*Source: AXCO Insurance Information Service*

# Kazakh Insurance Market Performance, FY2018:

*(in thousands Tenge)*

| | 2017 | 2018 |
|---|---|---|
| Insurance premiums | 396,321,524 | 384,845,926 |
| Net sum of insurance premiums | 266,584,863 | 295,009,964 |
| Assets | 925,335,292 | 1,048,509,862 |
| Capital | 411,696,356 | 468,266,501 |
| Authorized capital | 224,339,447 | 234,033,861 |
| Insurance reserves | 460,592,759 | 519,477,322 |
| Total Expenses | 267,180,101 | 290,292,955 |
| Net profit (loss) before corporate income tax | 67,184,788 | 94,514,371 |
| Net profit (loss) after taxes | 57,365,005 | 81,552,447 |

*Source: National Bank of Kazakhstan*

As of January 1, 2019, the Kazakh market was represented by 29 active re/insurers.

**Total GWP in 2018** decreased by 2.9% (from KZT 396.32 billion to KZT 384.85 billion). According to S&P Global Ratings, non-life market last year demonstrated a general decline by 11%. Among the reasons the agency pointed out the exit of some players from the market, improvement of competition, as well as activity of some insurance companies, affiliated with banking and corporate groups. However, the life sector demonstrated a noticeable growth of GWP (about 20%). S&P Global Ratings expects that in 2019 growth of the entire insurance market will most likely be affected by the life sector due to changes in legislation, tax incentives and introduction of investment insurance. Based on the total market ranking, in 2018 the largest amount of GWP was generated by EURASIA (KZT 68.57 billion vs KZT 55.19 billion a year ago). Khalyk-Life (KZT 51.03 billion) and Khalyk-Kazakhinstrakh (KZT 44.54 billion) ranked 2nd and 3rd. The highest growth rates were recorded by Khalyk-Kazakhinstrakh (65.5%), Nomad Life (62.2%) and Kommesk-mir (51.2%).

**Total market paid claims** in local currency increased by 7.26%. Paid claims increased only in non-life classes. A significant increase of paid claims was recorded in cargo (+172.04%) and also in property insurance (+120.3%). However, due to depreciation of TENGE against EURO, the market paid claims in EUR, to the contrary, dropped by 2.78%.

**In 2018 assets** of the Kazakh insurance sector increased by 13.3% y-o-y from KZT 925.34 billion to KZT 1.05 trillion, as allinsurance.kz wrote.
Total liabilities of re/insurers in 2018 increased by 13% to KZT 580.2 billion, and insurance reserves - by 12.8% (KZT 519.5 billion). Total equity amounted to KZT 468.3 billion (+13.7%).

Based on 2018 result, EURASIA was the leader in terms of assets' volume among the local insurers, the company's assets went up by 14.9% y-o-y to KZT 251.29 billion (~24% of all market assets). 2nd place was taken by KHALYK-Life (assets increased by 124.2%, to KZT 145.2 billion). The main reason for such a growth was the merger of Kazkommerts-Life. Khalyk-Kazakhinstrakh took the 3rd place in terms of assets (+123.4%, to KZT 115.48 billion), partially as a result of the merger of Kazkommerts-Policy. At the end of January 2019 Khalyk-Kazakhinstrakh was renamed to Khalyk.

**In 2018 total equity** of the insurers increased by 13.7% y-o-y. EURASIA is also on the top in terms of the equity capital size (+29.2%, to KZT 141.27 billion). VICTORY goes second (+13%, to KZT 86.68 billion), the 3rd one is Khalyk-Kazakhinstrakh (+105.9%, to KZT 48.11 billion). According to the experts of S&P Global Ratings, the return on equity (ROE) in 2018 amounted to 19%, while in 2017 it was about 14%.

**Total retained earnings of insurers in 2018** increased by 40.2%, from KZT 56.2 billion to KZT 78.8 billion. According to S&P Global Ratings, the biggest share in the profit structure of the insurance sector in 2018 was generated by investment income (+48%). Based on 2018 result, EURASIA became the most profitable insurer (its revenue jumped from KZT 12.96 billion to KZT 32.8 billion). The TOP-3 in terms of income include VICTORY (+49.2%, to KZT 8.03 billion) and Kaspi Insurance (-24.7%, KZT 4.69 billion). In general, 10 out of 29 local companies by the end of 2018 increased their income by more than 100%.

**Total insurance settlement expenses in 2018** increased by 7.26% to KZT 95.18 billion. The 1st place in terms of expenses was taken again by EURASIA (KZT 33.4 billion), followed by Khalyk-Kazakhinstrakh (KZT 10.21 billion).

**The average profitability** of the insurance market in 2018 also went up - from 6.3% to 8%. The 1st place in terms of asset efficiency was taken by Alliance-Policy with ROA of 43.5%. 2nd goes Kaspi Insurance (ROA amounted to 26.7%), and the 3rd - European Insurance Company with ROA of 20%. The lowest ROA in 2018 was shown by SALEM (-32,2%), Amanat (-1%) and TransOil (1.5%).

For more information

NATIONAL BANK OF KAZAKHSTAN
OFFICIAL INTERNET-RESOURCE

**Performance of financial sector**
Insurance sector

- **TOTAL REPORTS** https://bit.ly/2P2ZzIa
- **FINANCIAL PERFORMANCE** https://bit.ly/2NgxF8L
- **CURRENT STATUS** https://bit.ly/2KEYPo5

**XPRIMM Insurance Profile:**
**KAZAKHSTAN Market Overview:**
**Full Year 2017 & First Half 2018**
44 pages

https://bit.ly/2HYDVPJ


# قناة السويس للتأمين

# Suez Canal Insurance

SCI

تأسست عام ١٩٧٩

16569
Call Center

الثقة.. وراحة البال

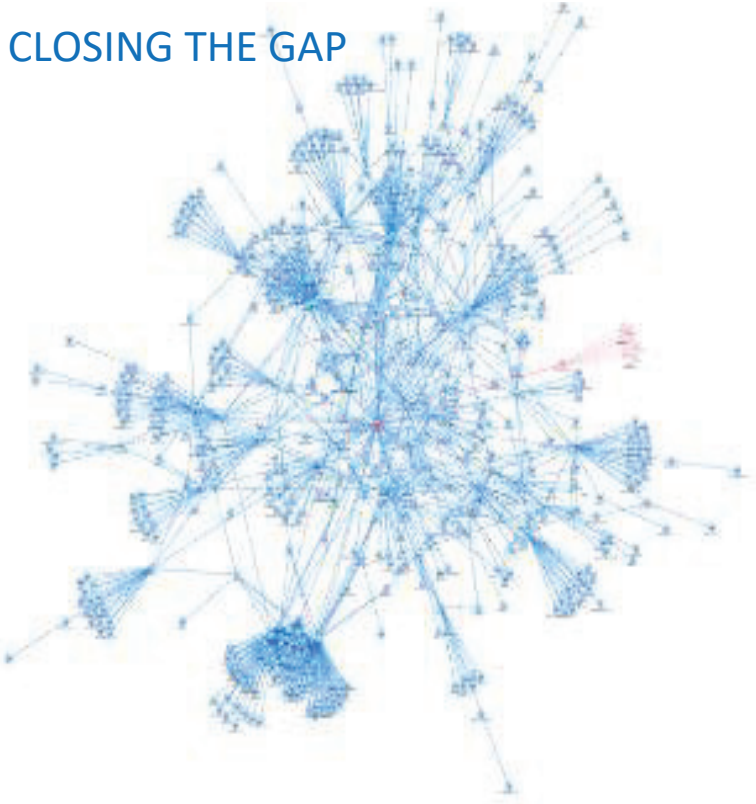
المركز الرئيسى : ٣١ شارع محمد كامل مرسى - المهندسين - الجيزة

تليفون : ٣٧٦٠١٠٥١ - ٣٧٦٠٦٨٦٨ فاكس : ٣٣٣٥٤٠٧٠ - ٣٣٣٥٠٩٨١

**2018 FAIR Case Study Competition Winner**

# CYBER INSURANCE & RISK MANAGEMENT:

## CLOSING THE GAP



Developed by: Lydiah N. Karanja
APA Insurance Ltd, Kenya

***The insights contained in this research work are purposely intended for this paper and the author's responsibility is limited to this presentation only.***

The objective of this presentation is to analyze the subject of cyber risk and effective methodologies of mitigating the effects of the said risk exposure.

## Introduction

It is paramount to first understand the meaning of the word cyber risk to enable us divulge into the insurance and appreciate the risk management aspect of cyber risk.

Cyber Risk can be defined as threat to an organization's digital information as a result of exposure and breach of network security system. Cyber Risk refers to vulnerability of a firm's information systems to fissures or attacks culminating in significant financial loss as well as stained brand reputation.

Cyberspace is a man-made environment created in the U.S. in the late 1960s, based on the developments of post-war technology.

The information system is the heart of any organization in the current era and is useful in running virtually everything about a firm. Right from the company website, storing sensitive medical data on all employees, trade secrets, processing of payroll, emails, telephone connectivity, customers and supplier records as well as online payments; All these are managed by use of the information system. Any threats to such a system will therefore be detrimental to the running of the entire organization by crippling all operations.

## Classifying Cyber Risks

Cyber risks can be categorized into two main classifications as expounded hereunder:

- Deliberate Malice. These are intended acts of well-orchestrated attacks by either external hackers or sabotage by irritated employees. This leads to infiltration of network, Denial of Service (DoS) which is unavailability of system for some time, extraction of intellectual property, business interruptions and poor performance of industrial and medical systems.

- Fortuitous Malice. These refer to accidental acts for instance human user error that can render the system temporarily unavailable, natural disasters like hurricanes. A third party whose system is connected could be experiencing system hitches which can spread to the firm's network and cause downtime.

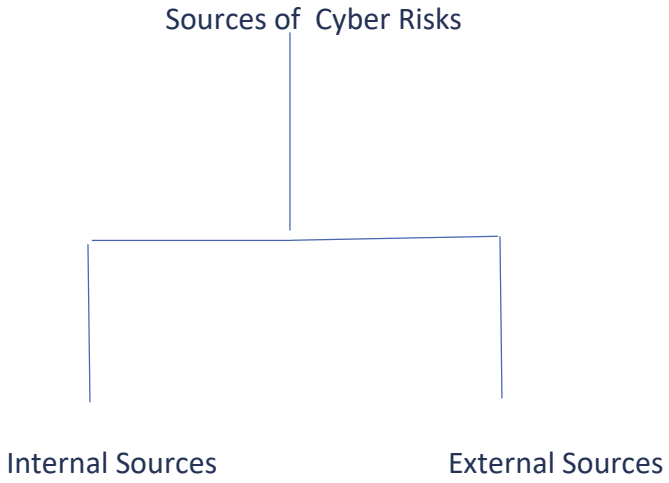
## How and Where does Cyber Risk originate from?

There are various sources of cyber risk which will be explained briefly here below.

- Lack of a cyber security policy that identifies threats and unauthorized activities, establishes and develops policies and oversight processes to protect company network and information.

- Mergers and Acquisitions done without conducting a thorough investigation into the target company's cyber history, and its cybersecurity infrastructure and policies.
- The world is a closely knit village as a result of globalization which leads to high threats to the cyber space linking states, corporations and governments.
- Outsourcing of business operations e.g. hired information technology system may pose a great risk to an organization owing to the fact that the supplier may not have a sound cyber security policy in place.
- Adoption of a new technology may pose a major threat in the process of digital migration, cloud integration and connectivity of new devices. During the process of transformation, the firm may find itself in an unfamiliar territory in terms of cyber security. Without clear assessments and interventions hackers will have an easy in through unpatched and outdated solutions, and unforeseen security gaps in newer technologies.
- Extension of third party network and relationships for instance a parent company allowing integration of its network with the subsidiaries and their intermediaries. Such a system tends to be poised for major attacks.
- Allowing a large number of staff to access highly confidential and sensitive company data.

Further, it is worth noting that cyber risks stem from both internal as well as external sources and their impact can be described as either quantitative or qualitative.



- Let's envision a scenario where a flash disk/laptop containing sensitive data is lost within an organization. The confidential data is stolen/deleted by a disgruntled employee. This leads to a series of hiccups at work ranging from inability to run debtors statements, process invoices, run basic day to day processes in the system, inability to pay suppliers, request for more replenishment of stocks, manage deliveries. This leads to big time downtime and unfortunately reaches the customers who start complaining due to poor customer service. Chances of false statements made on the website or social media are also high which leads to heightened efforts to recover the lost data. Additional cost is incurred and income and profits is lost due to systems downtime. All this time, production has greatly reduced, key employees are being poached by competitors, the market share of the firm has drastically dwindled and all the savings are now being directed towards saving the organization.

- On the external front, a third party can hack into the system and install a virus or disrupt the normal functioning of the system. All the efforts are geared towards saving the organization and at the same time the external environment which includes suppliers, customers, government, community and the media require an explanation on the happenings. All the while, the firm has suffered damage to reputation brand, shareholders start losing confidence in the current management leading to sacking of the CEO , the company starts to record drops in the stock market (if listed), at this point there has to be a profit warning issued, the stakeholders have now exerted extreme pressure on the management to streamline operations, due to loss of confidential data, customers can sue and the firm be penalized for negligence, likelihood of liability claims levelled against the firm are also high emanating from clients whose data is lost. False information spread on the website regarding a claimant could lead to a suit against the organization. In other instances, a third party can demand a ransom failure to which to damage the system or release stolen data.

**Historical Incidences of cyber attacks**

There are some notable Occurrences in the past that shaped the need for cyber risk management.

- Robert Tappan Morris and the Morris Worm (1988)- Creator of the first computer worm transmitted through the Internet where 6000 computers were reportedly affected causing an estimated $10-$100 million dollars in repair bills.

- The Melissa virus (1999)- a very simple virus which ended up costing $80 million in damages

- Solar Sunrise (1998)- systematic cyber attack was launched in the US which seized control of over 500 government and private computer systems.

-December 2015: A carefully designed cyber attack caused a power outage in Ukraine. 3-6h of black-out impacting 80.000 homes

-Feb 2016: Hackers stole $81M from Bangladesh national bank

-2015: Hackers stole $12M from Ecuador's Bancodel Austro

**How and Why do hackers go scot free?**

Cyber criminals have continued to enjoy some immunity for a long time due to several reasons:

- Attribution problem: it is almost impossible to gather conclusive evidence connecting a given individual to a cyberattack.

- It is difficult to bring cybercriminals to court, due to delays in international police cooperation procedures that are not compatible with IT speed, since evidence may be automatically erased after a few days or weeks.

-Most of the time the hackers could be located outside the legal jurisdiction of the court and prosecutors seeking the conviction. The prosecutors lack the legal powers to proceed with the suit. There are cross-boundary, reciprocal legal rules with many cyber allies, but many more countries don’t and won’t participate

-Having differences in interpretation of what is Lawful/Legal and unlawful/illegal for instance, if porn is illegal in a particular locality but is accessed on a computer that is located outside that locality, is it illegal? Is it prosecutable? Some local court systems say yes, but many more say no. For that reason, most smaller entities leave it up to the federal legal system to define and prosecute computer crime.

- The vast majority of internet crimes are never reported. Most people have no idea of where and how to report internet crime, and if they do, rarely does anything come of it. Because most internet crimes are not reported, accurate statistics and evidence are hard to come by -- even though they're needed to help in a successful prosecution.

-Gathering Legal evidence is a toll order as someone needs to address the following questions beforehand;

How can one confirm the log file hasn’t been tampered with?
Who had the ability to access the log file?
Is the time and date stamp accurate? How does one know?

How can one ascertain that the computer system accurately detected the originating IP address -- can't IP addresses be faked?
Was the log file originally written to write-once, read-only media?
What has been the chain-of-custody of that log file since it was first created until now?
What experience does the computer team have with obtaining legal evidence?

- Governments may even hire hackers for intelligence purposes, in exchange for protection against prosecutions for cybercrime.

**Burden of Cyber Risk**

The cost of cyber risks can be quantitative in the sense that they can be measured in monetary terms as listed below:
-Fines and Penalties
-Legal fees incurred in defense of law suits
-Reduced productivity as a result of poor sales
-Overheads which remain constant despite low production like salaries, bills, taxes.
-Revamped advertisements in an effort to salvage the company's image
-Penalties imposed by the government due to lack of compliance.

There are however some costs which can be difficult to quantify in monetary terms and can be termed as qualitative in nature:
-Loss of intellectual property
-Tarnished brand image
-Weakened market share/position
-Effect on a customer/third party who fails to meet their deadlines as a result of the organization's system interruption and is fined

Organizations globally are under extreme pressure from both the shareholders and other stakeholders to deliver on their mandate despite the threat of cyber risk. Firms have to maintain shareholders value, achieve new performance peaks, nurture employees to become topmost performers, satisfy customers needs, keep making new products and services as well as invest in communities.

***How then can an organization meet all the above expectations?***

The ultimate solution to this is in embracing Cyber Security best practices.

Unfortunately, the very essential strides that a company embraces to drive its agenda happen to be the ones that actually generate cyber risk threats.

It is worth noting that cyber risk cannot be totally exterminated, it can only be properly managed to ensure the smooth running of operations. The management needs to evaluate the following queries as they strive to embrace cyber security.

-To what extent can the company tolerate/retain any identified risk?

-How much is the organization willing to spend in terms of finances and personnel to manage the risk?

-In the unfortunate event a loss happens, would it be disastrous?

In terms of harm to employees, customers, suppliers, visitors, the public, brand image?

-Can the organization manage without technology and for how long?

The firm needs to make appropriate investments in security, vigilance and flexibility in order to ensure successful strategic growth and performance. This can only be effectively achieved if a company has a clear understanding of the threats facing the firm and their impact in the worst case scenarios.

**Positioning an Organization in managing Cyber Risks**

In modern business times, the success of any enterprise boils down to its ability to make informed decisions on cyber risk management. The business that is better positioned continues to enjoy continued growth whereas the firms that fail to embrace effective methods suffers dire consequences.

The various sources of cyber risks pose diverse levels of impact and this calls for prioritizing resources to manage and help mitigate likely outcomes. The areas to focus on are threefold:

-Organization internal organs: These are critical systems that contain the most sensitive data on all applications that help run all operations on the entire organization. Information on intellectual property, employees data, customers and suppliers information.

-Extended Information system: This could include supply chain management (SCM) applications, partner portals and systems extended to third parties.

-External systems like web pages and servers, systems accessible through the internet by the public.

The business needs to harness both tangible and intangible assets, human and financial and ensure compliance with policies and adherence to the legal and regulatory framework.

**Whose responsibility is cyber risk management?**

Management of cyber risk refers to the policies that counter vulnerabilities in information systems, programs and networks to ensure there is cyber security.

Since cyber risk is an area that touches more on information technology, it is assumed that the buck stops with the IT department. It is however the responsibility of every stakeholder in the business to ensure cyber security.

***"It is everyone's responsibility to ensure cyber security within an organization"***

Social networks and unlimited connectivity have seen to it that employees' work and social lives are no longer separate but have now been interweaved. Because of this, cyber security now rests with every employee to ensure their work and social data is safe.

**Ways to guarantee cyber security**

In today's world of immense cybersecurity risks, it is really important for enterprises to be pre-equipped with the security tools and privacy enhancements that are needed to safeguard their most valuable asset -data.

Outlined are ways to ensure cyber security:

-Educating employees on cyber security best practices.

-Regularly backing up the most important information like critical emails and shared data.

-Restricting user access. Employees are only required to access data they need.

-Securing networks by ensuring operating systems firewall is enabled. If employees work form remote access areas/ home, their home systems should also be protected by firewall.

-It's important to be cautious of clicking on any pictures on the internet, addresses, hyperlinks, pop-ups, ads and graphics. Some of them could be viruses and on clicking, the machine gets attacked.

-Running of anti-virus scans frequently and installing software updates regularly e.g once a month.

-It is very important to let anti-virus scans run to completion and allowing the system to reboot periodically.

-Limiting followers and access to social media. Employees need to beware of liking, following unfamiliar pages, or allowing different applications to access ones profile owing to the fact that not many internet users have proper cyber hygiene on cleaning them up when no longer required.

-Mobile users should password protect their devises, encrypt data and install security Apps.

-Being wary of public Wi-Fi by not selecting remember the Wi-Fi network. I addition, using the latest web browsers because they have improved security for fake browsers.

-Enabling privacy and security settings which are normally disabled on computers.

-Ensuring card readers are using modern EMV-chip technology which makes transactions safer

by creating unique transaction reference codes that cannot be used again.

-Limiting sensitive personal data on social media by only giving the basic information required to sign up accounts.

-Employing a password manager to help track the age of each password which ideally should be updated every nine months to one year. The password manager also assists in generating complex passwords for all accounts.

-Limiting social logins (single sign ons) where someone signs up for new accounts by using ones Google+ or Facebook.

-Desisting from providing one's passwords or personal information to unsolicited callers.

-Subscribing to identity protection

-Signing up for real-time alerts form the banks and credit card companies. This helps one track any unauthorized transactions in real-time.

-Routinely checking the credit card statements to determine if all purchases have been authorized by the owner.

-Using biometrics appropriately.

-Knowing one's digital footprint which refers to data that exists in cyber space as a result of actions and communications that one performs with others online.

-employing pinpoint to find the right technology partner of one's business.

-Using strong passwords and changing them periodically for instance every 3 months. A strong password should contain alphabets, numerical as well as special characters/symbols like @#!/.

-Performing daily full system scans.

-Creating a periodic system back-up schedule to ensure one's data is retrievable should an attack happen to ones machine.

-Regularly updating one's computer system to repair any bugs and abnormalities with the system.

-Installing anti-spyware and anti-malware software which specifically targets spyware and malware threats.

-Implementing the right technology that allows one to monitor third parties in real-time.

The above mentioned methodologies are internal policies and processes undertaken by an organization to safeguard its information system from cyber threats. By clearly identifying threats, a firm needs to understand what could happen should the threat materialize, proceed to quantify in monetary terms the cost of salvaging the effects of cyber sabotage. Ultimately, the organization needs to embrace effective cyber risk management practices and policies.

In addition to the above mentioned methods of enhancing cyber security, the firm needs to be properly positioned in terms of implementing cyber security controls to enable achievement of the targeted cyber security standards.

We now briefly list ways of implementing cyber security controls which will in turn guarantee cyber security which is the main objective of the organization.

- Having the ability to discover, identify and monitor all devices connected to the network. These may be all authorized and unauthorized devices like laptops, tablets and printers, sensors, IP cameras, heart monitors, infusion pumps. It's important to monitor the exact location of the various devices, their access restrictions, ability to detect abnormal behavior.

-Regular penetration tests within the company to gauge the organization's preparedness in countering attacks.

-Assessing data recovery ability.

-Ensuring secure configurations for network like installing firewalls

-Limitation and Control of Network Ports, Protocols, and Services

-Installing malware defenses

-Taking a detailed inventory of all authorized and unauthorized software connected to the network.

-Maintenance, Monitoring, and Analysis of Audit Logs.

-Ensuring limited number of users with access to privileged and highly confidential information.

-Continuous trainings to all users on ways to enhance cyber security.

-Ensuring emails and web browser protections.

The main objective of this coursework is to explore a cyber risk management method which is transfer of the risk through insurance which will be expounded on in detail in the following pages.

**Cyber Risk Insurance**

Businesses are different in terms of operations and so are the products/services on cyber insurance. Although there is no standard rule for underwriting these policies, the coverage offered normally cover two main areas;

-First Party Coverage- protects against losses suffered by the insured

-Third Party Coverage- protects against losses suffered by third parties.

Let's start by analyzing what is covered under first party cover.

- **Theft and Fraud**: This covers theft of data and extortion of the insured's funds. Unintentional distribution of the stolen data and trade secrets.
- **Investigation Costs**: A forensics investigation is necessary to determine the cause of loss of data, how to repair damage and how to prevent the same type of breach from occurring in the future. Investigations may involve the services of a third-party security firm, as well as coordination with law enforcement and the FBI.
- **Business losses:** A cyber insurance policy may include similar items that are covered by an errors & omissions policy (errors due to negligence and other reasons), as well as monetary losses experienced by network downtime.
- **Network and Business Interruption**. Covers the costs of business lost and additional expense due to an interruption of the insured's computer systems. Some cyber policies require that the interruption be caused by an intentional cyber attack and some do not. There could also be a requirement on time excess and cover is also subject to a set indemnity period.
- **Extortion**. Covers the costs of "ransom" if a third party demands payment to refrain from publicly disclosing or causing damage to the insured's confidential electronic data and intellectual property.
- **Lawsuits:** This covers legal expenses associated with legal settlements and regulatory fines.
- **Cost of Data Recovery:** This covers the costs of restoring lost data, diagnosing and repairing the cause of the loss.
- **Privacy Breach Notification:** Cover is provided for data breach notification to clients and other affected parties.
- **Repair of tainted company brand reputation:** costs associated with advertisements aimed at restoring back stained image.

We now look at the coverage offered to third party liability coverage.

- **Transmission of viruses coverage: C**over for liabilities arising from damage occasioned to third parties due to malicious virus transmission.

- **Notification costs:** Cover is provided to include costs of informing clients/third parties about data breach incidents. The cover here may limit the number of people to be notified and the means/modes of notifying them.
- **Governmental action**: Cover may be provided for any costs to be paid to the government for breaches of data, failure to adhere to regulatory measures and negligence-failure to exercise due diligence and protect the employees, clients.
- **Privacy liability cover:** This cover takes care of any liabilities arising from data breaches on employees, clients and suppliers private and sensitive information. The insured owes all these stakeholders a duty of care in ensuring their private data is well safeguarded.
- **Crisis Management:** Cover to strive to buy back the publics' confidence and trust after the fallout and try to mend ways. This extends to cover call centre charges

There are some important elements to take into consideration while signing up for a policy.

- **Choice of Counsel:** Insurers sometimes require the insured to only choose defense firms from their select panel of law firms to represent them in a legal suit. This is due to the substantial costs likely to be associated with a significant data breach case.

-**Trigger of a law suit:** Some policies will only respond if there is a demand letter or a suit levelled against the insured. This therefore means any defense that has not materialized into a suit is not covered.

-**Trigger of loss or a claim:** Some policies come into play if an actual loss or claim is made against the insured, event that triggers coverage is considered as well as the timing of the claim which will determine if the policy will respond or not.

-**Retroactive date cover**: Insurers normally limit their coverage to losses occurring after the retroactive date indicated on the policy which usually starts at inception of cover though an insured can negotiate for a date prior to inception at an additional premium.

-**Acts and Omissions of third parties:** If the insured relies on a system provided by a hired third party to store sensitive customers data, they (insured) need to have a cover that expressly extends coverage for data breaches occasioned by the third party system. Otherwise most of the policies will exclude breaches by such a system.

- **Unencrypted devices**: Coverage for losses emanating from machines whose data is unencrypted is normally excluded. It is therefore important to determine if cover is extended to cover such machines or not.

-**Policy Territory**: Majority of cyber policies limit their territorial scope to unites states of America. Coverage beyond the territory may only be granted at an additional premium. It is therefore important to understand the scope of the territory being covered.

-**Physical Location of breach**: Some policies only limit the location of breach to the insured premises only. This means virus attacks to laptops at home, while travelling, at the airport is not covered. Also theft of flash discs or external disks while one is travelling is not covered.

-**Acts or Omissions**: Some policies normally limit coverage for;

1. The insured's failure to take reasonable steps to design, maintain and upgrade its security

2. ) Defects in security of which the insured was aware prior to the inception of cover.

3. Certain malfunctions of security software.

-**Acts of War or Terrorism**: In some policies this is an exclusion but can be bought back to ensure liabilities arising from acts of hostile/foreign nation is covered.

There are some extensions that can be offered in addition to cyber risk the standard cover.;

-Publication of credit card information

-Extortion (Ransom)

-Electronic Theft for Instance Internet banking

- Multimedia Liability

-Monitoring

-Intellectual Property Infringement.

**Cyber Crime risk standard exclusions**

There are standard exclusions which are excluded in a standard crime liability cover. However, some of them can be bought back by way of paying some extra premium.

-Prior and/or pending claims

-Improvement Costs-Bettering the risk than it was previously

-Business Interruption that is not caused as a result of cyber related incidences

-Bodily injury and property damage

-Violation of patent rights

-Unlawfully collected data

-Unauthorized trading

-Contractual liability

-Employees mistakes or criminal acts.

**What's the Role of Insurance in the Cyber Domain?**

-Improve the understanding of cyber risks (and a data base pertaining to them) overcoming inhibitions to disclose/share). Identify trends

-Employ its risk underwriting potential to establish benchmarks for good cybersecurity practices.

-Incentivize compliance with these standards.

-Underwrite cyber risk beyond physical damages and loss of business due to service disruption to cover to IP and even reputational damages

- Help identify aggregation risks.

- Harmonize behavior across nations and corporations (which no nationlregulation or legislation can do)

**Areas of Interest to Insurers before providing cover**

Insurers would like to advance coverage to an organization that has a cyber risk profile. This is where the enterprise has analyzed its susceptibility to cyber attacks and has employed best practices to ensure any would be attacks are dealt with soonest possible and claims are minimized.

An organization that embraces employee trainings and awareness about cyber security is also likely to receive favorable terms and wider coverage.

An enterprise that conducts threat intelligence oftenly is better placed to be prepared to counter any possible cyber attacks.

An Insurer may require an audit of the company's processes, procedures and mode of governance. This gives an insurer some insight into cyber risk tolerance of the firm.

**Underwriting Challenges**

Underwriters need:

-An understanding of the Insured's business model in order to conceptualize the risk;

-Exposure data [of various types] in order to price the risk;

-Risk control information to assess the risk

-Sense of the loss context to undertake the risk.

It is important, particularly in the case of claims made on the eve of policy renewal, to precisely define which factual events trigger coverage. Current policy language is inconsistent, and most policies are on a claims-made basis, which increases the potential for mixed triggers (a claim could be filed when a loss is discovered, or when a system is compromised).

The industry needs to be able to more accurately value loss. Forensic investigation commissioned by or on behalf of the insured is meant to establish the cause and extent of a breach, but it does not address the financial impact on the insured.

The way clauses are applied also needs to be examined. A policy with primary coverage that has a war and terrorism exclusion with a buyback clause for cyberterrorism could include excess coverage that does not. This can result in disputes over payment of claims. Further, the utility of such clauses is limited due to difficulties with attribution.

There is discontinuity between primary and excess markets. There is no loss adjuster appointed on behalf of the market, which results in the primary insurer acting in its own best interest to the detriment of the underwriters of the excess coverage.

Cyber insurance is bundled into existing products. In order for the risk to be better understood and quantified, specific cyber products are required in place of silent coverage within existing products. Silent coverage is a significant problem because the potential cost could be considerable unless a policy has sub limits and clear wording. Simply adding clear cyber exclusions to policies, which might be difficult in this market to do that anyway, is inadequate in itself, since our customers require coverage.

Pricing models should be based on a close examination of the risk that needs to be underwritten and validation of the risk to the extent possible using available data. Conceptually, there is no barrier to developing pricing models around first-party dependencies and values, but most of the market is still using professional liability rates. If the industry does not have robust pricing models in place now, it will not be ready when it needs to transfer the pricing of cyber exposures into the automobile market, for example.

**Conclusion**

The insurance industry is going through a difficult transition in which we do not have adequate profitability to invest in new risk. We should be optimistic. The industry has tackled many new risks in the past, so we can tackle at least some of these new risks, as well as the traditional

risks that are regenerating. Our challenges are to obtain the right resources, adapt our culture, and offer reliable solutions that, at the same time, appeal to our customers and are viable for us over the long term.

A potential insured seeking coverage approaches an insurer and the it is a requirement to have a cyber risk proposal form completed to allow further negotiations. What is contained in a cyber proposal from?

**Cyber Risk Questionnaire/Proposal Form**

Outlined below are the common queries contained in a cyber questionnaire.

***1. Insureds General Information***

-Name of proposer/organization
-Physical Location-country, city, street, building. Addresses-telephone number, emails.
-Date of business establishment
-Details regarding any mergers/acquisitions and any such planned exercises in the near future.
-Any involvements in joint Ventures-Details on how all processes, procedures and policies have been integrated into the parent/main group system.
-An summary of the business activities carried out at the firm on a daily basis.
-The number of employees including casuals and contractors/sub-contractors involved.
-Details of revenue generated in the last financial year, current and projected gross income in the following year.

***2. Data Information***

-Details on the number of data records stored in the system-basic personal employees data, sensitive information on employees health, firm's trade secrets, payment card information, financial as well as third parties like clients, suppliers, debtors, the government and adjacent community.

-The proposer is required to disclose if employee/client data is shared with third parties, whether it is anonymized prior to sharing, for what purposes is the shared data used for.

-What due diligence the proposer takes to ensure the recipient of the shared data has cyber secure environment.

***3. Network Exposure***

-The amounts generated via online platforms in terms of sales, commissions, donations, Fees.
-The level of fluctuations in the online revenues and by what percentage. At what point the revenues are at the highest.

-In case of any network disruption, the amount that would be at stake at any given time.
-What steps the Insured takes to prevent big time outages like having a back-up system
-The additional costs that would be incurred to minimize the impact of disruption.
-Any disaster recovery plans and processes.

***4. Third party Exposure (***outsourced service provider-OSP)

-Information on Data services outsourced to third parties.
- What due diligence is undertaken before engaging with a new outsourced service provider
-How data is stored-whether in private cloud or in shared servers.
-If data breach occurs, whose responsibility is to do notifications and who bears the costs?
- If an OSP system or cloud service is unavailable, what is the likely impact on the insured
-The business recovery measures in place following cloud failure.

***5. Data Security***

**-**Monitoring of sensitive data on the network
-Whether the confidential data stored on the servers/data bases is encrypted when stored and during transmission
-Whether critical data is backed-up at least weekly.
-Whether the insured maintains back-up tapes/cassettes/disks
- Access to highly sensitive data is only given to very few senior staff upon authorization.
-Whether there is a Chief Privacy Officer or who runs that function.
-Details on compliance with various bodies like Health Information Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach Bliley Act (1999), Fair and Accurate Credit Transactions Act (FACTA), Payment Card Industry Data Security Standards
-Description of data retention and destruction policy.
-Whether the insured maintains user revocation procedures on user accounts following employee termination.

***6. Network Security***

-Whether the insured utilizes firewalls, Anti-Virus or Anti-Malware
- Network access controls for remote access
-Whether the insured enforces a 'strong password policy' requiring passwords of adequate complexity and length.
-Confirmation of carrying out server and application security configuration hardening
-Whether the organization maintains a Whitelist to prevent malicious software and other unapproved programs from running
-A description of the process of managing and installing patches on systems and applications
-Use of any unsupported operating systems or software

-Disablement of USD drives to employees
- Whether the organization has a Social Media presence

***7. Security Policies and Procedures***

-If the insured has a cyber-threat intelligence gathering function
- Is regular penetration testing carried out by a 3rd party? When last performed, any serious concerns raise on the last one carried out and what remedial steps have been taken to address such concerns
-Maintenance of any certified information security standards.
-Any regular security assessments carried out by a 3rd party? When last performed, any serious concerns raise on the last one carried out and what remedial steps have been taken to address such concerns
-Any continuous awareness training programme for employees regarding data privacy/security, including legal liability and social engineering issues
- performing of background verification checks for all candidates of employment, contractors and 3rd party users

***8. Points of Sale (POS) and Merchants (Only for users of credit cards for Payments)***

-Confirmation of being fully compliant with EMV card processing standards
-Whether the POS systems have anti-tampering features
-Confirmation that the POS devices regularly scanned for malware or skimming devices
-Requirement for formal approval to changes to the POS systems
-Information on whether POS network assessed by a 3rd party
-Any high level vulnerabilities on the POS system and how they have been addressed.
-Whether the POS system developed and maintained by a PA-DSS compliant vendor
-Description of how payment card data is captured and transferred to the credit card processor, including the encryption and/or tokenisation process
-Whether changes on individual files on the POS system create alerts in real-time
-If the POS systems have anti-tampering features

***9. Incident Response and Claims History***

-Any incidences in the last 5 years relating to;

-Unauthorized disclosure or transmission of any confidential information

-Negligent or unintentional act or failure to act by an employee or an employee of any third party service provider whilst operating, maintaining or upgrading the computer system.

-suspension or degradation of the computer system

- Your inability to access data due to such data being deleted, damaged, corrupted, altered or lost

-Any receipt of extortion demand or security threat

- Receipt of a claim in respect of any of the above

- Any formal or official action, investigation, inquiry or audit by a regulator arising out of the use, control, collection, storing, processing or suspected misuse of personal information

-Whether the insured has any incident response plan which includes a team with specified roles and responsibilities and if it has been tested in the last 12 months.
-If the Insured maintains incident log of all system security breaches and network failures

***10. Limits of Liability Required***

The limit of Liability requested will be determined by the level of exposure foreseen, the system controls in place and any history of loss incidents. It follows that a higher limit will see the insured pay relatively higher premium due to the high risk being transferred to the insurer.

The Insured then consents to the declaration by appending their signature, company stamp and date. The proposal form is then forwarded to the insurer to be analyzed and revert with terms and/or their advises.

The Insurer can offer coverage for a cybercrime policy based on 2 primary policy forms;

-Claims Occurring basis

-Claims made basis

- A cyber crime policy on a claims occurring basis meets claims that occur during the policy period regardless of when the claim is made. It covers claims that have occurred during a period of cover even if the claim is made after the cover has been lapsed or cancelled.
- A policy on Claims Made basis meets claims that are made and reported during the policy period for work undertaken after the retroactive date shown on the policy. The Retroactive Date is usually the date at which cover was first incepted. At each renewal the same Retroactive Date is carried forward. This cover will not provide cover for any claims after a policy has been lapsed or cancelled as there is no policy in force when the claim is made. It is therefore important to consider purchasing a ‘run off’ cover. This will

cover claims after the lapsing or cancelling arising from work occurring prior to lapsing or cancelling.

**A different Perspective on Cyber Insurance**

Cyber insurance is not unique as a product. It covers losses that exhibit similar patterns to certain others covered by standard insurance. Indemnification for data loss notification or event management is not that different from the product recall coverage that might exist as an extension in some product liability policies. Cyber extortion is not dissimilar to kidnap and ransom in terms of indemnification process and service provided to the insured. Computer fraud could be covered by a crime or fraud policy.

The indemnification principle for Business process disruption due to an IT network interruption is similar to the one for Business Interruption following a property damage. Data or computer restoration costs are not unlike replacement costs of any asset covered by a property policy. Privacy or Security liability claims are substantially similar to an E&O claim.

First, cyber risks are strongly linked to intangible assets, which represent a growing portion of every company's assets. For this reason, the insurance market must focus more on how to value and insure data and intellectual property, and how to quantify reputation damage and determine whether or not it can be insured.

Second, non-physical losses are commonly covered, but we must ensure that the industry has the expertise to indemnify business interruption due to a cyberattack without material damage. We must also face conflicting interests that may exist between criminal investigation and preservation of evidence on one hand and prompt business recovery on the other hand.

Third, we must be ready to cope with the very dynamic threat landscape in which risks are not only increasing, but also changing in nature. This includes increasingly pervasive technology. With connected objects, cyber risk is now entering the physical world, and attacks may result in material damage, bodily injury, and circumstances that are currently covered by existing policies. We need to examine whether standard policies are able to respond to this risk.

Finally, systemic risk is a key issue and risk propagation is an intrinsic feature of cyber risks developing in an interconnected world. We must explore how to manage the accumulation of risk due to common vulnerabilities or cascading effects.

We have so far addressed cyber risk insurance and our next move will focus on cyber risk management.

## Cyber Risk Management

**Definition**: Risk Management is the process of identification, analysis, assessment, control, avoidance and minimization of cyber risk exposure within an organization.

The enterprise needs to assess the likelihood and potential impact of a cyber risk exposure and then determine the best approach to deal with the risks. Given that cyber risk cannot be entirely eliminated, risk management should come into play in tackling the effects of uncertainty on organizational objectives in a way that makes the most effective and efficient use of limited resources.

First and foremost, the organization needs to be aligned with its main goals and objectives which sets the right foundation for effective risk management process. The company needs to adopt a cyber risk strategy which addresses six main key areas.

- Identification and assessment of the firm's tangible and intangible core assets.
- Develop a cyber risk appetite i.e. Determine what magnitude of risk the firm is willing to accept and retain.
- Assessing the profile of cyber attackers or in a nutshell find out the likelihood of cybercrime damage that would be suffered should it happen.
- Based on point number 3 above, the firm needs to assess their preparedness and defense strategies in mitigating cyber threats.
- Measurement and Quantification-This is estimating the severity of possible cyber threats in monetary terms.
- Having clearly analyzed, assessed and quantified the effects of a cyber threat, it is important for an enterprise to consider the best response methods in managing cyber risks e.g. risk retention, transfer (Insurance), loss mitigation measures (educating staff).

## Considerations for Effective Risk Management Process

- Speedy response: Response to counter attacks should be timely in terms of early detection, speedy mitigation measures taken and recovery plans. This calls for thorough preparedness.
- Elasticity: An organization should endeavor to continue operating during and after the disruptive periods. It should withstand tough market times and deliver on its mandate amid the operational stress and disruption.
- Continuous Trainings: The Organization needs to embrace a culture of regular trainings to enhance cyber security throughout the company.
- Communication Processes: An enterprise needs to have clear lines of detecting threats, communicating the same to the relevant personnel who in turn take the necessary

action and if the matter seems out of hand, to escalate the same to higher authorities. All through, all staff should be kept in the know how on what's happening.

- An Organization should have its priorities right owing to the fact that there are limited resources in terms of staff and funds. Prioritizing enables the company allocate adequate resources towards managing cyber threats.
- Investing on Intelligence: The company requires to engage in continuous intelligence tests to enable timely detection of any cyber threats both internally and externally. Some cyber penetration tests should be carried out frequently to establish the level of preparedness in countering any possible threats.
- Maintaining cyber hygiene: Implementing basic cyber hygiene practices is a good starting point for cyber risk management. It aids in timely detection of threats, effective reduction of any impact should there be any attack.

***How can an organization maintain Cyber Hygiene?***

The Center for Internet Security (CIS) defines cyber hygiene as a means to appropriately protect and maintain IT systems and devices and implement cyber security best practices.

There are various ways that can enhance cyber hygiene as outlined below;

-Making use of complex passwords that contain a minimum of 8 characters ranging from numerical, alphabetical, symbols and special characters.

-Limiting the number of users with access privileges to highly sensitive and confidential data.

-Blocking installation of new software by users without prior approval from the head of IT department.

-Continuous trainings to all staff on ways of maintaining cyber security like always logging off their machines after work, locking the machines when not in use for some time, ways to identify potential phishing efforts.

-The company should maintain a record of all hardware and software on the organization's network.

- Identify vulnerable applications that aren't in use and disable them.

-Making sure data is always backed up and having several copies of the same data to enable one access the original copy should there be any threat to the system.

-Adoption of Industry's accepted configurations standards like NIST and CIS benchmark.

-Patching all applications immediately and regularly to minimize incidences of attacks.

-Ensuring the system is always upgraded to newer versions as the aging ones have already been well mastered by potential hackers.

**Five steps of cyber Breach Response Escalation Plan**

- Pre-Breach Response Planning

- Identify Internal Response Team & Incident Lead Person

- Establish Analysis and Communication Protocol

- Complete Data Breach Response Plan

- Evaluate Vendor and Customer Notification Requirements

- Remediation and Recovery Vendors

- Stress Test Response Plan

- Fraud Prevention

- Incident Analysis

- Contact the Team

- Identify Information (Payment Card compromised)

- Breach Containment

- Harm Determination Forensic Analysis

-Legal Analysis

- Security Breach Incident Analysis

- Incident Disclosure

- Analyze Requirements

- Consider Alternative Notice Methods

- Notify in compliance with laws

- Consider third-party vendors for notification

- Stagger Notification

- Public Reporting

- Cyber Insurance Carrier Notification

- Loss Mitigation

- Credit Monitoring

-Fraud Monitoring

-Documentation and discoveries manifest

-Customer Service

-Human Resources

  - Communication and Remediation

-External Solutions

-Customer protection and notification letter

-Customer hotline number establishment

-Breach website

-Senior management updates

-Human Resource updates

-Cyber Insurer briefing

-Directors and Officers Liability Insurer briefing (If Material)

-Limit Communication

**Question 1:**

**How Your company managed to protect itself against different types of cyber risks.**

An Insurance company is an organization that handles massive amounts of data ranging from the prospects/proposers' personal information, Insureds personal details, employees' data, suppliers, debtors and creditors information as well as third parties details.

Such a huge organization cannot run the daily operations without the assistance of an information system to aid in data processing, storage and transfer of information. This therefore means such a company can be a major target for cyber attack owing to the vast amount of data contained in the system.

There are measures taken by our organization to shield the enterprise from cyber attacks which will be highlighted below:

- Continuous training of staff on various ways to minimize cyber risk attacks. Below is an excerpt of a circular done by the head of IT to all staff mid 2017.

***"CYBER SECURITY ALERT***

*Dear team,*

*In an effort to further enhance our company's cyber defenses, we want to highlight a common cyber-attack that everyone should be aware of – phishing. "Phishing" is the most common type of cyber-attack that affects organizations like ours. Phishing attacks can take many forms, but they all share a common goal – getting you to share sensitive information such as login credentials, credit card information, or bank account details.*
*Although we maintain controls to help protect our networks and computers from cyber threats, we rely on you to be our first line of defense. We've outlined a few different types of phishing attacks to watch out for:*

- *Phishing: In this type of attack, hackers impersonate a real company to obtain your login credentials. You may receive an e-mail asking you to verify your account details with a link that takes you to an imposter login screen that delivers your information directly to the attackers.*
- *Spear Phishing: Spear phishing is a more sophisticated phishing attack that includes customized information that makes the attacker seem like a legitimate source. They may use your name and phone number and refer to APA in the e-mail to trick you into thinking they have a connection to you, making you more likely to click a link or attachment that they provide.*

- *Whaling: Whaling is a popular ploy aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real company executive. Using a fake domain that appears similar to ours, they look like normal emails from a high-level official of the company, typically the GCEO, CEOs or CFOs, and ask you for sensitive information (including usernames and passwords).*
- *Shared Document Phishing: You may receive an e-mail that appears to come from file sharing sites like Dropbox or Google Drive alerting you that a document has been shared with you. The link provided in these e-mails will take you to a fake login page that mimics the real login page and will steal your account credentials.*

***What actions to take….***

*To avoid these phishing schemes, please observe the following email best practices:*

- *Do not click on links or attachments from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types.*
- *Do not provide sensitive personal information (like usernames and passwords) over email.*
- *Watch for email senders that use suspicious or misleading domain names. There is currently a lot of spam (unsolicited emails) going round. Do not open these emails if you cannot verify authenticity of the sender.*
- *Inspect uniform resource locators (URLs) carefully to make sure they're legitimate and not imposter sites.*
- *Do not try to open any shared document that you're not expecting to receive.*
- *If you can't tell if an email is legitimate or not, please do not open the email and contact IT support for assistance.*
- *Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.*

*Thanks again for helping to keep our network, and our people, safe from these cyber threats. Please let us know if you have any questions."*

- In addition to point 1 above, the Organization has invested heavily in back-up servers that guarantee availability of data should there be an attack and data is lost.
- There is a fully fledged IT department that is mandated with the responsibility of ensuring any cyber threats are addressed in a timely manner.

- The company has ensured installation of anti-virus, anti-malware and anti-spyware on all machines of staff.
- There is a requirement to change all users' passwords every three months and no password can be used more than once. The passwords have to meet the company's set standard of complexity in terms of length-minimum of eight characters, inclusion of special characters e.g. @#!.
- There is also limited access to highly confidential and privileged information on trade secrets, company assets, employees' health records.
- All emails sent using the company address have a disclaimer which states as under-" *This e-mail, including attachments, is intended for the person(s) or company named and may contain confidential and/or legally privileged information. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited. If you are not the intended recipient, please delete this message and notify the sender. Please note that any opinions, express or implied, presented are solely those of the author and do not necessarily represent those of APA Apollo. Every proposer whilst seeking new insurance or renewing an existing Policy must disclose any information which might influence APA in deciding whether or not to accept a risk. The proposer is solely responsible for any information provided. Failure to make appropriate disclosures may render the insurance voidable from inception and enable APA to repudiate liability on claims presented. Unless advised otherwise, it is understood by APA that the proposer or insured is acting on their own behalf and has appropriate authority to do so. All incoming and outgoing e-mail messages are stored in our Mail Archives. If you do not wish the retention of potentially private e-mails by us, we strongly advise you not to use the APA Apollo e-mail accounts for any private, non-business related communications."*
- Once an employee attempts to log in to a machine and they use incorrect password, one is allowed to attempt a minimum of 3 times after which one gets locked out and can only be reset again by IT personnel.
- Staff are only allowed to access necessary data on their line of duty that is stored on shared networks. For instance, there could be Underwriting folder, Marketing, Claims Medical insurance and agriculture folders. If a staff works in finance department, they are restricted from accessing all the above mentioned folders as they do not need the information contained therein.
- Once an email is sent to any user within the organization that could have some virus, any attachments on such an email do not open and one is referred to IT for assistance. This means there is timely and effective detection of cyber viruses.
- There are restrictions on what sites the company's browser can log onto. If a user attempts to search an unauthorized site, the browser will give a warning and one cannot proceed.
- Staff are also restricted in terms of using flash disks, CD players and connecting any external systems to their machines without consent from head of IT.

- All staff machines have the same wallpaper and no staff is allowed to install features of their choice. There is a standard wallpaper and background colour.
- Machines automatically log off/lock after 10 minutes if not in use and when one resumes, it is a requirement to log in again using one's password.
- The IT staff routinely take an inventory of all machine on the network at any one point. No machine is allowed to log onto the network without being approved by the head of IT.
- When an employee leaves/ceases work, their password, log-in credentials are disabled/deactivated and no one can use them to log onto a machine.
- The organization has embraced use of newer application versions like windows and word 2016.

There are some challenges to overcome as the organization strives to enhance cyber security.

- Need to raise cyber expertise in the Organization.
- Improvement of Risk Management process and quality of information
- Collection of data & Building of risk models
- Manage risk aggregation and exposure to Cyber Cat

Once the above noted challenge are addressed, the company will be better placed to enjoy some benefits as outlined under.

- Offer tangible solutions to clients.
- Leverage digitalization to enhance company's operations
- Become a player among the best Insurers in the market
- Improve knowledge and market share on cyber risk.

**Question 2:**
**New products of Cyber Insurance for specific industries (Supply chain, Banks, Petrochemicals, Hotels, etc)**

The uniqueness in industries in terms of operations calls for customized cyber policies to cater for the needs of each segment. There is no standardized approach on cyber insurance which means that the product offered to like a bank might differ with one offered to a restaurant, hospital or a Legal firm.

We shall briefly address some few select industries by highlighting the ideal coverage suitable for such an industry.

- **Banks:** On 10th April 2018, there was a statement issued jointly by the Federal Reserve, FDIC, OCC, NCUA and CFPB through their affiliation in the Federal Financial Institutions Examination Council (FFIEC) alerting banks of risk management issues regarding cyber insurance coverage.

The regulators did not require banks to take up cyber insurance but it did propose consideration of uptake of the cover to take care of some losses stemming from customer identity theft, fraud and even extortion. These losses would result in income decreases, lawsuits, regulatory fines and reputation damage. Each bank is to involve multiple stakeholders within its organization for example, legal, risk management, IT and financial staff to review the bank's existing control environment and related cyber risks.

Banks normally take up Bankers Blanket Bond policy to cover majority of its risk exposure under one umbrella and at times there can be an extension on BBB to cover cyber risks or it can be taken as a stand-alone product.

The management of a bank should consider the following factors before settling on any cyber insurance product:

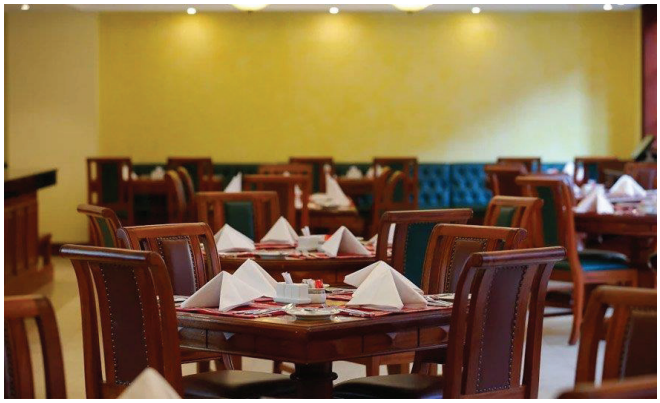
-Identify loopholes for cyber threats and sample some coverage that can address such gaps.

-Get to fully understand what will be the triggers of losses covered, the sub-limits, exclusions on the policy and the premium chargeable.

-Before effecting cover, it is important to find out if the Insurer is well capitalized and of good claims paying ability history.

-It is important that the management of the bank understands that taking up an insurance policy does not mean that they are absolved of their mandate to continuously enhance cyber security within the organization.

- **Hotels:** The hospitality industry is highly dependent on electronic processes and computer networks in the daily operations to aid in marketing their facilities, online bookings and payments, they also gather and maintain private information about their clients. The hospitality industry also engages vendors, contractors and third party service providers.



*A typical dining area in a restaurant*

Some of the cyber risks associated with this industry emanate from;

-Payments by use of credit cards
- Disclosure of Personal identification information while booking hotel rooms
-Points of sale machines
-Online payments for hotel bookings
-Employee Information on personal details
-Third Party Information-Suppliers, vendors and contractors.

The ideal cyber insurance coverage for hotel industry can be divided into 2 policies:

- First Party Coverage: As earlier on explained in this paper, first party coverage extends to cater for the following risks:
  -Loss of income due to failure of network security
  -Network business interruption
  -Data restoration costs
  -Response management costs associated with public relation consultants to assist in restoring the tainted brand image, Forensic costs, call Centre/notification costs
  -Cyber Extortion
- Third Party Coverage: This covers the following;
  -Liability arising out of defamation and infringement of intellectual property rights.
  -Fines and Penalties arising out of privacy breach regulatory proceedings

- Failure of computer network security to guard against threats such as hackers, viruses, worms, Trojan horses and denial of service attacks whether or not resulting from the provision of professional services.
- Wrongful disclosure of Personally Identifiable Information, Protected Health Information or confidential corporate information in the client's care, custody or control via a computer network or off-line.

- **Petrochemicals:**


The oil, gas and petroleum industry has not been spared from cyber threats/attacks. It is important to look into 2 areas while addressing industrial cyber risk.

- Information Technology (IT): relating to computing technology such as networking, hardware, software and internet. This combines all computer abilities to collect, process and present information for decision making purposes across a business organization.
- Operational Technology (OT): Industrial Control System (ICS) which support physical value creation in manufacturing processes largely in the form of automation. The ICS comprises all necessary hardware and software to control and monitor process equipment.

The ICS includes the following;

-Supervisory Control and Data Acquisitions Systems (SCADA) – used throughout the oil, gas and petrochemical industry to display information from controlling systems to the plant operator through a human machine interface (HMI), in some industries such as pipeline operation the SCADA will also be used for its control functionality

-Distributed Control Systems (DCS) – again used throughout the oil, gas and petrochemical industry for facility control, alarm and in some cases emergency shutdown purposes (i.e. Integrated Control & Safety Systems (ICSS)). DCS systems are optimized to handle high volumes of complex process logic

- Programmable Logic Controllers (PLC) - used for equipment specific control and safety functions such as emergency shutdown (ESD), either standalone (local) or communicating to DCS or SCADA. For a PLC being used for a critical ESD function the safety instrumented systems (SIS) is optimized for speed and reliability.

Cyber attackers can target the following areas;

-Equipment Sabotage: A hacker could implant false data showing that there had been a breakdown in the equipment in a remote facility, leading the victim company to waste time and financial resources investigating.

- Plant Destruction: A cybercriminal could engineer an oil explosion by increasing the maximum filling limit of an oil tank.

- Oil Market Fraud: Malware can fake data about the amount of oil a company has in stock to make the quantity appear much bigger than it actually is. Once the victim company runs out of oil, it won't be able to deliver to its customers. Failure to satisfy its obligations could wreak havoc and lead to changes in oil prices, as well as huge losses to the company.

Here are some of the risks a company may face in the case of a successful attack:

-Undetected spills

-Utilities interruption

-Production circle shutdown

-Inappropriate product quality

-Equipment damage

-Safety measures violation resulting in injuries and even death

-Plant shutdown

There is need to establish good general IT security procedures for the ICS, these should include the following:

-Backing up control system software

-Controlling access to engineering workstations

-Controlling access to the ICS

-Blocking USB and / or other access points to the ICS

- Management of mobile devices

The firm should also invest heavily in a cyber risk insurance policy to cater for unforeseen costs like business losses, investigation costs, network and business interruption costs, extortion of funds, privacy breach notification and other coverage as earlier mentioned in this paper.

- **Supply chain:** It is important to understand the context of a business supply chain i.e. what the environment the business operates in dictate about cyber risks- product's use, what it is connected to, and who the users are.

  - How the product will be used; The focus is on what type of data will be managed in the system. Essentially, the company needs to determine the consequence of the data being compromised or leaked outside of the system.
  - How the system is connected to the rest of the world; A system that is connected to the public internet will need more reliable security, since it would be easy to find and attack. On the other hand, a system that is isolated from any other network would have a much lower risk of attack or data breach, since the attacker would need to be in physical proximity of the system.
  - Who the system users are; Are the users internal employees who are trained on security procedures, or is the system accessed by a public user base which may not consider risky security behaviors? Simple security procedures, such as keeping passwords secret and maintaining current anti-virus software, cannot be counted on if the management does not directly control the users' environment.

  It is also important to dig into the developers' coding practices, whether the developer has ensured enough safeguards are in place to prevent the discovery, or exploitation of vulnerabilities in their apps or software.

**Premeditated & Political Challenges to Promoting Interstate Cyber Norms**

-Broad, generic, cultural divides in attitudes toward norms
-Complexity of issues, and diversity of domestic stakeholders
-Conflicting visions over utility, indispensability, and cost/risk associated with cyber weapons and warfare
-Fundamental divergence over what constitutes cyber warfare (versus information security): linkages & priorities
-Number and diversity of pertinent players internationally

-Complexity of issues associated with handling non state actors (proxies, private sector entities, NGOs, criminals)

Offensive action by States can contribute to cyber insecurity. Code is left behind after a cyberattack, and the victims can learn from this and retaliate. However, when confronted with a choice between traditional and cyber warfare, the latter may be a more attractive option for States. Such acts could serve a legitimate national security purpose when used – selectively and responsibly – not only for intelligence, but also for offensively targeting equipment in wartime situations. In the current climate, governments must not launch attacks lightly. Several factors could encourage major players to show restraint, including ethical and legal concerns, their own vulnerability to retaliation, the difficulty in accurately identifying foes (misattribution), fear of blowback (systemic effects), and fear of compromising their own capabilities or sources.

While conflicts and crime are increasingly being channeled into cyberspace, States and institutions are weakening. States are under pressure, challenged, and often unable to regulate within their own territories. If States do successfully regulate internally, without international agreement, their rules may be ignored, sidestepped, or interpreted in widely different ways. There has also been a significant increase in companies offering offensive services to States or corporate clients: those who have significant technological, operational and financial capabilities are developing their skills and offering. These actors are operating in countries where rules are lax and engaging in offensive cyber operations is tolerated.
Perhaps the most serious issues we are facing going forward are the general undermining of confidence and trust, and the manipulation of integrity of data, which is rare, but increasingly worrisome.

**On the Private Sector Front….**

For technology companies like Microsoft, governments are both major customers and Advanced Persistent Threats (APT). Companies must maintain a relationship of trust with governments through transparency and neutrality. It is essential that governments understand that the role of technology providers is not to take sides in the geopolitical debate. Their sole interest in this context should be cyber defense and security.
Governments need to be smarter about procuring information technology, and they need to spend more money to update it. It is also imperative that companies invest in cybersecurity, although certain factors will remain beyond their control, such as users failing to update or upgrade software. The cloud offers a viable alternative to maintaining and securing in-house IT infrastructure. It can offer significant advantages, such as stronger security models and redundancy.

**What's the Role of the Government in enhancing Cyber Security?**
Governments should be at the fore front in implementing programs to increase the cybersecurity of organizations and to assist in the aftermath of attacks. Governments are offering incentives to companies to beef up their security, or assisting them in doing so.

Governments have put in place mechanisms whereby certain organizations can call on outside Computer Emergency Response Teams (CERT) to assist with response or mitigation if they believe they have been attacked by a state.

It is of utmost importance for governments to develop and implement a Cybersecurity National Action Plan that spells out actionable plans to be undertaken by a well funded body to mitigate the effects of cyber risks.
It is the role of the government to come up with legislation on cyber security and enforce its adherence by all stakeholders within a country. Hefty fines and penalties should be levied organizations that fail to meet the minimum requirements.

The government can in addition to the above outlined responsibilities rollout a cyber awareness campaign, extend the campaign to learning institutions by implementing a subject to be examined in all learning institutions.

Every day, cybercriminals carry out large-scale economic surveillance to undermine the competitiveness of companies. These attackers, who come from a wide range of origins, infiltrate IT and communication networks to steal important or vital company information. They often start to lay the groundwork for their attacks with social engineering, which is manipulating or tricking people into revealing information or performing some action. They have access to people and a great deal of information that is freely available online, particularly through professional social networks like LinkedIn. On such sites they can obtain information on strategic projects, employee responsibilities, technologies used, and identify vulnerabilities they can exploit.

**Sabotage**

Acts of sabotage can constitute acts of war or terrorism, and this is the case in an international security context. However, it is easier to attack Critical National Infrastructure (CNI), such as mass transport, banking systems and power grids, than it is to attack military targets. An attack on CNI could have devastating effects. The consequences of the shutdown of a national power grid or water distribution system would be dire: beyond the economic impact, there would also be loss of life.

A business needs to invest heavily in business risk intelligence which covers the broader risks to the organization, ranging from insider threats to the physical security of executives and staff, or the risk of engaging with third-party vendors in the supply chain.
Finally, the Organization should adhere to the set guidelines on its cyber security strategy.


Malaysian Re

**Financial Strength Rating of 'A' Strong ( Stable Outlook ) by Fitch Ratings**
**Financial Strength Rating of 'A-' Excellent ( Stable Outlook ) by A.M. Best**

**MALAYSIAN REINSURANCE BERHAD** (664194-V)
(A wholly owned subsidiary of MNRB Holdings Berhad)

www.malaysian-re.com.my

MALAYSIAN RE

# FAIR Medical Insurance & Healthcare Congress

## "World of Opportunities"

## 22 - 24 July 2019

## Paradise Island Resort & Spa

# Maldives

Allied Insurance Company

Under the patronage of the Governor of Maldives Monetary Authority, and Health Minister of the Maldives **H.E. Mr. Abdulla Ameen**, and in collaboration with Allied Insurance Company of the Maldives, FAIR successfully held the first conference of the Medical Insurance and Healthcare Congress under the theme

"A World of Opportunity"

The conference was held at the Paradise Island Resort & Spa in Maldives on 22-24 July 2019. The conference was attended by delegates from 10 countries representing 35 companies and associations from various Afro-Asian insurance markets. They exchanged views and experiences in the developments of the medical insurance market. The conference's speakers were specialized in Medical Insurance, Reinsurance, and Insurance Brokerage, and gave dynamic sessions included interaction between them and the attendees, covering five topics:

- Government Health Insurance Scheme
- Fraud , Waste & Abuse
- Reinsurance and High-Risk Pools: Past - Present and Future Role in Individual Market
- Role of Private Insurance in implementing Public Universal Health Coverage
- New Roles of Brokers in Health Insurance


This essential Medical Insurance and Healthcare event gathered a wide range of the industry's leaders from all around the globe, starting with **Dr. Adel Mounir**, FAIR Secretary General, **Mr. Mohamed Shafaz**, Managing Director of Allied Insurance Company of the Maldives, **Dr. Ehab Abul-Magd**, the Congress Excecutive Manager, and **Mr. Hussen Amr Mohamed Rashad**, Managing Director and C.E.O of State Trading Organization, in addition to delegates from more than 35 companies and associations from various Afro-Asian insurance markets attended the conference.

**Dr. Adel Mounir** in his opening speech, noted that the FAIR Medical Insurance and Healthcare congress was established under FAIR umbrella, to be a platform that gathers world distinguished Healthcare experts and business, enhance the awareness and provide technical assistance in the field of Medical Insurance & Healthcare. In addition to act as a technical arm supporting the activities of Medical Insurance & Healthcare management in the local & multinational companies in Afro-Asian Region.


H.E. Mr. Abdulla Ameen


Mr. Mohamed Shafaz


Dr. Adel Mounir


Dr. Ehab Abul Magd

## • Government Health Insurance Scheme

Mr. Ibrahim Firshan

Mr. Niyaz Mohamed

Ms. Aminath Zeeniya

Ms. Mariyam Shafeeq

The first session was titled "Government Health Insurance Scheme" and moderated by **Mr. Ibrahim Firshan**, General Manager at Allied Insurance.
Speakers were: **Mr. Niyaz Mohamed,** Chairman of the Board of Directors at Aasandha, **Ms. Aminath Zeeniya**, Assistant Manager at Aasandha, **Ms. Mariyam Shafeeq**, Managing Director at Aasandha.

They introduced the definition of Health Insurance as it is concerned with access to health care and financial protection against the risk of incurring very high expenditures for such care, while Social Health Insurance is a government-sponsored insurance program, where risks are transferred to and pooled by an organization, often governmental, that is legally required to provide certain benefits.
The session then gave a brief about the history of SHI in Maldives, and an introduction of Aasandha, which is a national social health insurance scheme for all the Maldivians which covered health services to a maximum of MVR 100,000 per head per year, and a premium of MVR 2,750 was paid per person by the Government for whole population. Under this scheme, all the government hospitals, health centers and one private hospital were included to provide health insurance service to Maldivians, Health services which are not available in the Maldives were covered by sending abroad i.e. Sri Lanka & India. The Scheme operated on a fee-for-service direct billing arrangement with providers and did not require beneficiaries to make any payment if the costs were within the specified annuals limits and are covered under the Scheme. The Scheme belongs to the National Social Protection Agency (NSPA), and under an understanding it was handed over to Aasandha Company to implement it. Ponting out that Aasandha is a Private Limited is a State-Owned Enterprise (SOE) Company which compromise of 100% share by the Government. The Scheme is administered by Aasandha Company under the governance of Aasandha Scheme Board and policy guidance of NSPA. All scheme related policies and procedures are formulated by NSPA (endorsing service providers, service types , prices, etc.).


## • *Fraud , Waste & Abuse*

Dr. Sherif Fathy Youssef

Mr. Anil Nair

The second session was moderated by **Dr. Sherif Fathy Youssef**, Chairman &CEO of Inaya Egypt Healthcare Administrator.
The speakers was: **Mr. Anil Nair,** CEO of IRIS Health Services LLC.

**Mr. Anil** explained What exactly is Fraud , Waste & Abuse (FWA),
Fraud: intentional concealment or deception to gain something of value (e.g. Billing for services at an inflated rate).
Waste: excessive use of health services, although not necessarily intentional wrongdoing (e.g. Prescribing a medically unnecessary procedure based on comfort level).
Abuse: practices that are inconsistent with accepted sound fiscal, business, or medical practices, and result in an unnecessary cost or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care. Unsubstantiated payment for services, sometimes intentional, exploiting gaps in policy (e.g. Misusing codes on a claim).

He gave examples of Healthcare fraud as Misrepresentation of the type or level of service provider, Billing for items and services that have not been rendered, Seeking increased payment or reimbursement for services that are correctly billed at a lower rate (up-coding), Misusing codes on a claim "THERE ARE WAYS TO ROOT OUT WASTE…..
but it requires a continuous cycle of intervention and standardization. Most payer organizations live in a type of limbo — let's call it the "wasteland.""
He said,
He pointed out that Payers need to develop robust mechanism by deploying latest technology , experience and expertise to: Detect, Diagnose, Reduce, Prevent

He added that Not all FWA cases are intentional, A good number of these are mere inefficiencies and unintentional errors that unfortunately, lead to duplicate tests and incorrect billings.
Reason : Dense, complex billing and reimbursement system that health.


## • *Reinsurance and High-Risk Pools: Past –Present and Future Role in Individual Market*

The second session was moderated by **Dr. Adel Mounir**, FAIR Secretary General.
The speakers was: **Mr. Mohamed ElDishish,** Reinsurance Expert.

Policymakers are currently considering proposals to strengthen insurance markets and risk pools by establishing a reinsurance program or similar market-stabilizing mechanism. Such programs work by reimbursing health insurance providers a portion of the medical costs associated with providing coverage and care to high-cost and high-risk individuals.

**Mr. Mohamed** shared his perspective and insights about state experiences with reinsurance programs and examined program design and policy considerations, discussing the importance of the Reinsurance role in improving and strengthening the capacity of insurance markets, expressing the developments occurred within the reinsurance sector, and pointing out how reinsurance can be essential to the individual markets.

Dr. Adel Mounir

Mr. Mohamed ElDishish

Session Three


## • *Role of Private Insurance in implementing Public Universal Health Coverage*



Mr. Abdul Wahid Thowfeeq

Dr. Ehab Abul Magd

The Fourth session was moderated by **Mr. Abdul Wahid Thowfeeq**, Managing Director of Dhivehi Insurance.
The speakers was: **Dr. Ehab Abul-Magd,** the Congress Executive Manager, Chairman & MD of Platinum Healthcare Holding Group.

**Dr. Ehab** talked about the Currant Public Health Insurance System in Egypt, pointing out that the social health insurance system (HIO) in Egypt has been in existence since 1964, and it was the outcome of many legislations started in the early decades of the 20th century.

He expressed the Strengths of Current HIO as there is a big number of OPDs & Hospitals owned by HIO, it has enormous expertise in Health Insurance. HIO is considered as a reference for Health Insurance in the region, HIO Hospitals are accredited training centers by EFB, ABHS, RCSI & Cairo Faculty of Medicine.
While challenges Facing HIO are such as incomplete coverage, multiple Laws & Systems, unrealistic rates of premium, low revenue collection rate, Opt out strategy, unclear Benefit Package, continuous advances in Healthcare Industry, technology & Knowledge Revolution.

Solutions to overcome those challenges are Purchaser/Provider SPLIT, moving from Passive to Strategic purchaser, unifying the Laws, compulsory scheme, subsidization of poor, no opt out, design Benefit Package.

He defined Universal Health Coverage (UHC) as it provide ALL people with access to needed health services (including promotion, treatment, rehabilitation, and palliation) of sufficient quality to be effective, Ensure that the use of these services does not expose the user to financial hardship"
As for Challenges & UHC Approach , it is categorized into Structural/Stewardship, Resources, Financial, Service Delivery. And overcoming those challenges can be through New UHI Law (2018), which features Population Coverage ALL, Payer Provider Split, Public Private Partnership, Defined Benefit Package, Complete Fiscal Autonomy, More Cost Sharing.


## • *New Roles of Brokers in Health Insurance*

The Fifth session was moderated by **Mr. Vivek K. Naik**, PRINCIPAL OFFICER / DIRECTOR of Synergy Re Specialist (Labuan) Ltd.
The speakers was: **Mr. K.L.Naik,** Chief Consultant of Synergy Re Specialist (Labuan) Ltd.

**Mr. K.L.Naik** stated that health insurance aims to protect all citizens, poor-n-lower middle class who cannot afford to buy insurance.

He continued that under such a scenario, 'modicare' of our prime minister is a ray of hope with massive health insurance schemes covering more than 100 million families i.E. More than 500 million plus population of lower middle and poor classes of our society! It has become a reality of life that **Health Insurance Schemes** Like **Ayushman Bharat** Are **For** The People**, Of** The People**, By** The Welfare States Governments. 'Modicare' is a new word for all kinds of healthcare- medicare services available at hospital chains on cashless basis i.E expenses are reimbursed directly by government funding to service providers of healthcare.
He pointed out that an insurance broker is to reach grass roots levels of our society to bring common man on massive scale of lower middle and poor people who cannot afford insurances. All these segments of society are to be brought in the main stream of insurance protections for them to insure and be secure, adding that new role of health insurance brokers is to be played with a missionary zeal to arise, awaken and strengthen common men in their struggle to live a better life with good health- mental, physical and social.
They represent insureds to insurers and give their contribution by technological and marketing skills.
Insureds are laymen, insurance brokers provide insurance technological knowledge to handle risk management and claims management of all insureds, they have expertise to manage experts with 'know who' and ' know how' to negotiate better deal with insurers with insurance policy terms to cover risks of all insureds.
They make analytical study of various innovative products of many insurers.Health insurance brokers and health insurers create teams of dedicated spectialists. 'Team' is a term without 'i' – ego of any one.


Mr. K.L.Naik


Mr. Vivek K. Naik

Session Five

# FAIR Events for 2020

## Mark Your Diary

- FAIR Risk Management Conference


- FAIR Medical Insurance & Healthcare Congress

- FAIR Reinsurance Forum

ARAB RE

# Staying up-to-date makes a difference

To keep you informed of the must-to-know industry-related news and events, Arab Re goes beyond traditional reinsurance boundaries by bringing to you its

## News App


- Relevant Daily News from all over the world
- Our Corporate News and Events

Available on the App Store

ANDROID APP ON Google play

**Tune-in to panoramic news and download our new App**


RE_
SILIENT
Fire harnesses the strength within us to stand strong
and forge a bright future, even in the face of adversity.
It fuels our passion to deliver nothing but the very best
to all our clients.
Trust Re. Inspired by the elements.
WWW.TRUSTRE.COM
TRUST RE
REINSURER OF CHOICE