



# FAIR Review

Issue No. 180 - June 2019

## Morocco

A Sophisticated African Insurance Market





**SCR**

CRÉATEUR DE RÉSILIENCE DEPUIS 1960

RESILIENCE BUILDER SINCE 1960

# 26<sup>TH</sup> FAIR CONFERENCE MARRAKECH - MOROCCO

SEPTEMBER 23<sup>RD</sup> - 25<sup>TH</sup> 2019

NEW ECONOMIC BARRIERS IN AFRO ASIAN INSURANCE MARKETS



[www.fair2019.com](http://www.fair2019.com)

# FAIR Review

## FAIR in Brief

Federation of Afro-Asian Insurers & reinsurers “FAIR” is a price-less 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 prompting 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.

The articles in FAIR Review represent the opinion of the authors and are not representative of the views of FAIR. Responsibility for the information and views expressed lies entirely with the author(s).

## Issue No. 180 June 2019

### **Secretary General**

Dr. Adel Mounir

### **Editorial Consultant**

Mr. Hussein ElSayed

### **Media Manager**

Mr. Ahmed Sirag

### 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



## FAIR News

4



## Global News

8



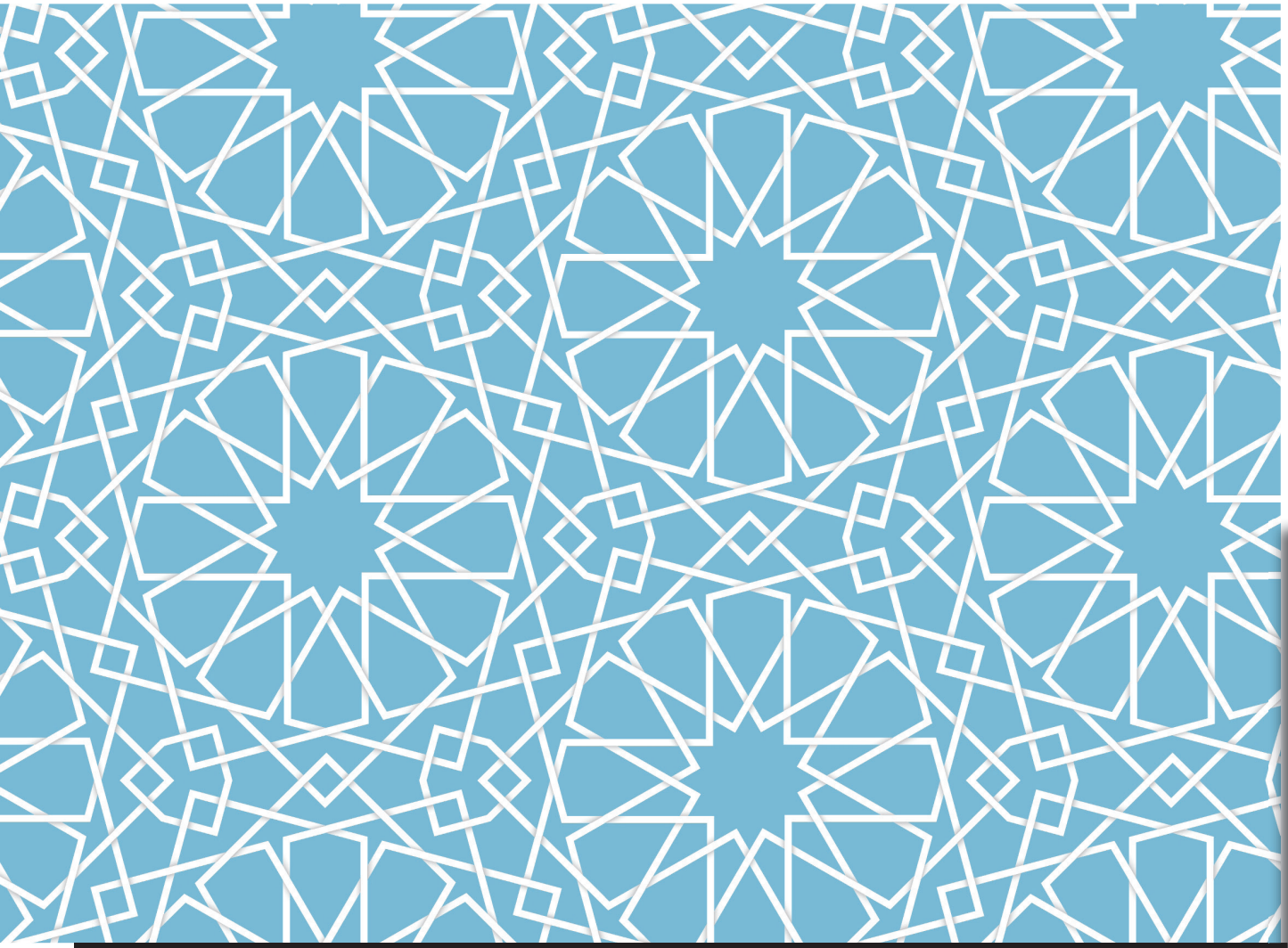
## Africa News

23



## Asia News

35



## Country Profile



45

## Cyber Insurance And Risk Management: Closing The Gap



59

# FAIR News



## • **1st BIMTECH-FAIR International Seminar**

In collaboration with FAIR, The Birla Institute of Management Technology (BIMTECH) held the 1st BIMTECH-FAIR International Seminar on:

### **“Capitalizing On The Emerging Trends In Insurance In Afro-Asian Region: In Quest Of Profitable And Sustainable Growth”**



The Seminar was held during 23 - 24 April 2019 at Radisson Blu MBD Hotel, Delhi-India. Several eminent personalities from Egypt, Bangladesh, UAE and India came together to discuss and analyze the emerging trends in Insurance and the various problems and throw up solutions by keeping in mind sustainable growth along with profitability of Afro-Asian countries.

#### **Seminar Key Topics were:**

- Making Life Insurance Protection Accessible to All.
- Health Insurance Protection – An opportunity to Expand Access.
- Insurtech: Have they been upto the challenge?
- Reinsurance: Coping up with the worsening Nat Cat environment.



# 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

• **FAIR Training on Engineering Insurance**



In coordination with **The Association of Ethiopian Insurers** (represented by its chairman **Mr. Yared Mola**), **FAIR** (represented by **Ms. Heba Fouad**, FAIR Assistant Secretary General) held training on Engineering Insurance on 2 & 3 May 2019 at Intercontinental Addis Hotel, Addis Ababa-Ethiopia.

This training was attended by over 45 delegates from all insurance companies in Ethiopia.

The Training was given by **Mr. Mesfin Abebe**, Senior Manager - Underwriting & Marketing , Nairobi Regional Office, Africa Re, and **Mr. Ramesh Viswanathan**, Senior Underwriter - Engineering, Trust Re, Bahrain, and was covering :

1. Technical aspects of Infrastructure project
2. Underwriting and technical controls of Infrastructure projects
3. Advanced Loss of Profit
4. Two video clipping on construction of Wet Risk
5. Machinery Breakdown
6. Machinery Loss of Profit;
7. DOS - Deterioration of Stock

**Mr. Mesfin Abebe**

Senior Manager - Underwriting & Marketing , Nairobi Regional Office, Africa Re



**Mr. Ramesh Viswanathan**

Senior Underwriter - Engineering, Trust Re, Bahrain





**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](http://www.misrins.com.eg)

# Global News



## • **Global Insurance Market: At a crossroads**

**Allianz Research** has published its report entitled «Global Insurance Market: At a crossroads», a study which focuses on the state of the global insurance market in 2018 and outlines the outlook for the future.

According to this report, the global insurance premiums (excluding health) reached 4 180.56 billion EUR (4 180.56 billion USD) in 2018, an increase of 3.3% over one year and of 3% in a decade.

Life insurance reported 2 258 billion EUR (2 582.68 billion USD), representing a growth of 2.54% compared to the turnover achieved in 2017 (2 637.7 billion USD). Non-life insurance amounted to 1 396

billion EUR (1 596.73 billion USD) at the end of 2018, increasing by 4.65% against 1 334 billion EUR (1 597.95 billion USD) achieved one year earlier.

The American insurance market is the first premium producer with 1 115 billion EUR (1 275.33 billion USD). The Chinese market is far behind with 417 billion EUR (476.96 billion USD).

The American continent generates 32.86% of the global premium volume, that is 1 201 billion EUR (1 373.69 billion USD). Western Europe achieves 1 2 billion EUR (1 146.08 billion USD) and Asia 1 199 billion EUR (1 371.41 billion USD). ■



Charts and tables  
on life and non-life insurance markets

 **DATA ON SELECTED INSURANCE MARKETS**

<https://bit.ly/2WdD5HI>

 **GLOBAL INSURANCE MARKETS**

<https://bit.ly/30SwUam>

### • **The Geneva Association: Health protection gaps in emerging markets**

There is a broad consensus that private health insurance is preferable to out-of-pocket spending which can be financially catastrophic for households. With the right regulatory framework, private health insurance can have an important and beneficial effect on the sustainability of health schemes to which individuals, governments and employers contribute. The Geneva Association's Dr Kai-Uwe Schanz provides some insights.

People in emerging markets have great difficulty funding their healthcare needs, as overall expenditure in healthcare is growing faster than GDP. The share of healthcare expenditure has risen globally over the last two decades from about 8% to almost 10% of aggregate GDP. In emerging markets, higher healthcare costs are driven both by communicable diseases and by lifestyle-related diseases.

However, in these markets, the global trend of higher healthcare expenditure has not led to increased penetration of private health insurance, which remains insignificant with a 2% share of total healthcare expenditure.

The research paper 'Healthcare in Emerging Markets: Exploring the Protection Gaps' published by The Geneva Association analyses the health protection gap as out-of-pocket spending that is financially stressful for households.

Based on assumptions on the relationship between stressful out-of-pocket spending and per capita income, the association estimates the annual health protection gap in emerging markets at about \$310bn or approximately 1% of these countries' aggregate gross domestic product.

#### **Quantifying the gap**

Our estimate assumes that 100%, 75% and 50% of out-of-pocket spending in low-income, lower middle-income and upper middle-income countries, respectively, can be considered financially stressful and, therefore, is part of the health protection gap. This approach, however, disregards protection shortfalls as a result of lacking access to or the affordability of health services.

There is a broad consensus that private (voluntary) health insurance is preferable to out-of-pocket spending, which is the most inequitable and economically inefficient form of funding, with potentially catastrophic financial implications for households. If properly regulated in order to address potential market failures such as adverse selection and moral hazard, private voluntary health insurance can make an important and beneficial contribution to the sustainability,



quality, availability and cost-efficiency of health services in a multi-pillar system.

### **Private sector has a role to play**

Policymakers in emerging markets can harness private insurance as a catalyst for a socially-beneficial and economically-efficient transition to pooled pre-funding of healthcare expenses, including public, private and public-private schemes.

This contribution will become even more attractive to society as the role of private health insurers is shifting. They are evolving from payers of claims and benefits – as well as underwriting data collectors – to an expanded service proposition as providers of comprehensive healthcare advice and solutions. The structural challenges facing emerging markets' healthcare systems suggest that PVHI as a meaningful

component of future-proof healthcare systems can no longer be ignored.

### **Funding options**

Generally speaking, there are four main healthcare financing systems:

- social insurance, based on tax-like contributions and managed or regulated by governments;
- funding through tax revenues and other government resources;
- private direct payments (out of pocket); and
- private health voluntary insurance (Mehrotra and Delamonica 2005).

These categories are not mutually exclusive as all health systems represent a mixture of various elements. For example, mandatory health insurance requirements can be met through private health insurance, which, in turn, often contains elements of cost sharing such as co-payments or deductibles in order to discourage moral hazard and overuse of medical services.

Ultimately, consumers and employers pay for healthcare, either directly or through taxes. Having said this, the configuration of funding channels has important implications for income and wealth distribution.

### **New healthcare propositions in emerging markets**

In underpenetrated lower-income countries in particular, healthcare stakeholders are looking at technology to help



address some of their biggest challenges, such as prohibitive cost, poor quality of data and services, insufficient access and low awareness.

Advanced analytics and digitalisation have led to a dramatic increase in the amount of data, information and insight available to private health insurers, enabling them to achieve quantum leaps in patient care, especially in emerging markets.

The rise of electronic health-care data, in combination with unprecedented computing power and inexpensive data storage, greatly enhances the measurement of treatment outcomes and costs in a timely, accurate and cost-efficient manner. In addition, we are witnessing a surge in patient-generated clinical data, particularly from IoT devices. Digital connectivity is facilitating the sharing of this data between consumers and caregivers.

In future, insurers will have to offer a customer experience that is commensurate with what policyholders find elsewhere. For health insurers the prompt payment of claims and benefits will remain the necessary condition for staying relevant to customers.

However, an equally important condition will be to move beyond being a funding channel towards becoming an attractive and flexible risk partner that can contribute to improved health outcomes. As

well as risk cover, customers want their loyalty rewarded, and they demand enhanced ease and transparency in their dealings with insurers. Having said this, the most important additional customer requirement is arguably prevention, with insurers offering ways to lessen the impact of calamities that adversely impact the lives of policyholders.

If this vision of a greatly expanded value proposition comes true, the perception of private health insurers will fundamentally change for the better, positioning them to make a meaningful contribution to narrowing today's and tomorrow's health protection gaps.

### **Private voluntary health insurance**

Healthcare expenditure is set to continue outpacing economic growth. In low-income countries cost dynamics are driven by the rapid growth of chronic diseases in addition to traditional communicable diseases, which remain a formidable challenge. At the same time, as the majority of populations live in (remote) rural areas, the expansion of healthcare coverage requires increased spending. In the wealthier emerging countries, a combination of spreading critical illnesses, increasing service expectations of middle-class patients, investments into new devices and technologies and the effects of accelerating ageing are pushing up expenditure.

In light of the significant differences in quality among emerging market health systems, protection gaps need to be approached from two fundamentally different angles. The first perspective focuses on financially stressful spending in the presence of relatively well-developed medical infrastructures. A second approach, relevant to the majority of emerging countries, is based on the lack of access to and quality of health services as the most important issues, with a more immediate link between protection gaps and health outcomes such as life expectancy at birth.

From a public policy point of view, private voluntary health insurance can help expedite progress towards governments' main objective - to mitigate their populations' vulnerability to (catastrophic) out-of-pocket spending. Given huge informal economies and underdeveloped and inefficient taxation mechanisms in many emerging markets, private voluntary health insurance may be the best possible starting point or backing for any public or semi-public prepayment and risk pooling scheme. As historical experi-

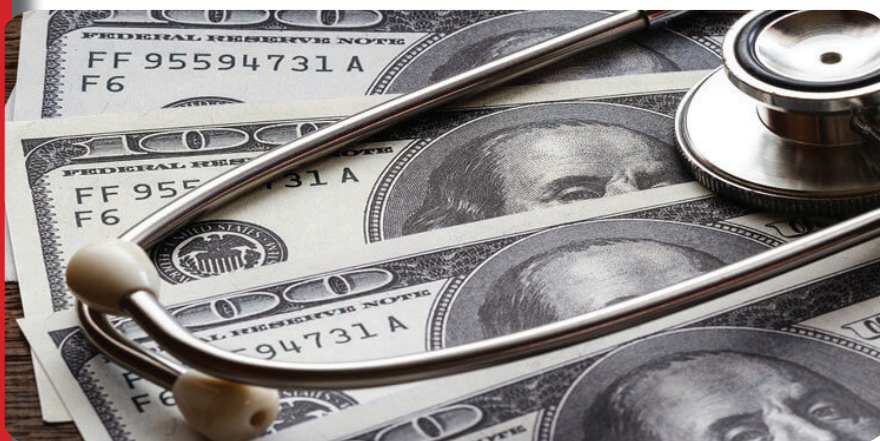
ence from Europe suggests, private voluntary health insurance can pave the way for the establishment of fully fledged publicly financed systems at a later stage.

For customers at the base of the economic pyramid, the small incomes from which premiums must be paid require insurers to come up with highly cost-efficient solutions. In addition, insurers need to cater to remote locations, low levels of education and a general lack of experience with formal institutions. Strategies for effectively overcoming these challenges include a radical simplification of products (including enrolment and claims submission), unconventional distribution channels such as telcos or farmer cooperatives, leveraging digital channels and entering into private-public partnerships such as the joint management of (compulsory) insurance schemes.

Healthcare funding is one of the biggest societal challenges of our time and the insurance industry can play a major role in offering sustainable solutions. A

Dr Kai-Uwe Schanz is director of the protection gap research programme at The Geneva Association. ■

Source: Asia Insurance Review | May 2019



## • *Reinsurance Trade Barriers and Market Access Issues Worldwide*

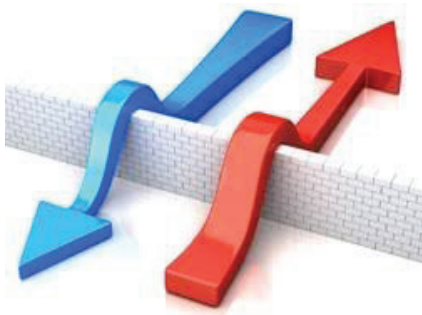


Global Reinsurance Forum (GRF) members account for more than 65% of global net reinsurance premiums. The GRF believes that positive and significant economic benefits will result from the free global flow of risk through open and competitive reinsurance markets.

The GRF has identified 45 major territories including regional groupings around the world which have either implemented, or are in the process of implementing, barriers to the transfer of risks through global reinsurance markets. This edition of the GRF document includes countries which had not been included in previous editions, but nonetheless implement barriers to the free flow of reinsurance across their territories and have come to our attention. Despite this edition of the GRF trade barriers report encouragingly showing that no new major barriers have been introduced since the last edition in July 2018, it remains concerning to see that significant existing barriers still remain in place worldwide. The failure of international gov-

ernments to include language in a joint-statement on the dangers of protectionist barriers during the G20 Summit in Buenos Aires is worrying and disappointing, particularly as G20 Summit statements in the past have consistently argued against protectionism. Such barriers reduce competition leading to reduced customer choice, higher reinsurance costs and less capacity over the long-term horizon. These reinsurance trade barriers and market access issues include but are not limited to:

- Restrictions on the ability of reinsurers to freely conduct business on a cross-border basis, thus limiting the capacity of global reinsurers to spread risk globally and to prevent domestic concentrations of risk. Varying levels of restriction are witnessed or developing in Algeria, Argentina, Azerbaijan, Brazil, China, Colombia, Ecuador, Egypt, Germany, India, Indonesia, Malaysia, Nepal, Nigeria, the Philippines, Poland, Singapore, South Africa, South Korea, Tanzania, Thailand, Vietnam,



as well as the groupings of other member countries of the African Union and the grouping of the Conférence Interafricaine des Marchés d'Assurances.

- Requirements for reinsurers operating on a cross-border basis to collateralise or localise assets, preventing the global reinsurance market from transferring and spreading risk on the basis of a competitive, level playing field across borders. Such requirements exist or are evolving in jurisdictions including Argentina, Brazil, Canada, China, , Israel, Portugal, Singapore, and the United States.
- Restrictions on foreign ownership of subsidiaries and other barriers to the establishment of branches, subsidiaries and operations. This restricts the ability of reinsurers to deliver their full economic benefit by providing local underwriting expertise and direct services to transfer risk out of domestic markets on an open and competitive basis. Such barriers are present or developing to varying extents in a number of jurisdictions including, but not limited to: Algeria, Argentina, Azerbaijan, Bangladesh, Brazil, Cambodia, China, Egypt, India, Indonesia, Kenya, Malaysia, Moldova, Nigeria, Russia, Saudi Arabia, South Africa, UAE, UK and the U.S.
- The use of discriminatory and anti-competitive mechanisms such as compulsory cessions to domestic entities, systems of 'right of first refusal', and compulsory, subsidized or monopolistic governmental mechanisms limiting the competitive capacity of global reinsurers to operate on a level playing field. Such practices concentrate risk domestically, whilst limiting customer choice, and can be witnessed or are developing to varying degrees in the African Union, Algeria, Argentina, Bangladesh, Belarus, Brazil, Cambodia, China, Colombia, Ecuador, Egypt, Ethiopia, France, Gabon, India, Indonesia, Kenya, Malaysia, Namibia, Nepal, Nigeria, Pakistan, the Philippines, Russia, Saudi Arabia, Senegal, Sri Lanka, Sudan, Tanzania, Vietnam and elsewhere.

**Developments since the last edition of this document was published**

- On 12 December 2018 the Indian insurance regulator, IRDAI, issued its Reinsurance Regulations which came into effect on 1 January 2019. The new Regulations confirm the enforcement of the Order of Preference Regulations 2016 and set out the procedure to follow for reinsurance placements. The order of preference itself is now referred to as the 'Offer for Participation'



and maintains that 'Indian reinsurers' are given first refusal i.e. the General Insurance Corporation.

- On 17 December 2018, the Saudi Arabian Monetary Agency (SAMA) issued licensing and supervision rules for foreign insurance and reinsurance companies wishing to establish and operate a branch in the Kingdom, including capital adequacy and financial suitability for obtaining a licence.
- A draft US-UK Covered Agreement has been prepared and awaits legislative approval in both the US and the UK. Its provisions are consistent with the US-EU Covered Agreement signed in 2017. See details of the US-EU agreement later in the document.

*The GRF continues to encourage jurisdictions to remove existing and remaining barriers to reinsurance. Such improvements will be in the interests of governments, policyholders, taxpayers and national economies. ■*



<https://bit.ly/2IU0iY6>

### • **EIOPA reveals priorities for 2019 and insurance stress-test recommendations**

The European Insurance and Occupational Pensions Authority (EIOPA) has revealed its priorities for 2019. These encompass new supervisory activities including work on conduct of business supervisory practices under the Supervisory Handbook, analysis of the consistency of technical provisions best estimate calculation, analysis of the supervision of run-off undertakings, as well as the promotion of supervisory convergence in the European pensions sector regarding the implementation of IORP II.

The priorities are set out in EIOPA's 2018 Supervisory Activities Report, which outlines the supervisory activities conducted in 2018 and sets out the priorities for 2019.

It states that in 2018, EIOPA addressed supervisory convergence from different perspectives and using different tools, depending on the issue and risks at stake. "In 2018, supervisory activities contributed to high-quality supervision, to enhanced convergence of supervisory practices and to stability in the European insurance sector," says EIOPA in the report.

EIOPA also says it will improve the follow-up of EIOPA recommendations addressed to the National Competent Authorities (NCAs), "and continue to assess supervisory practices in general and on a themat-





Gabriel Bernardino

ic basis to foster supervisory convergence and consistent, high-quality supervisory practices among NCAs for the benefit of the European citizens”.

EIOPA also published its 2018 Insurance Stress Test Recommendations. The recommendations consider the risks and vulnerabilities identified through the findings of the ‘2018 Insurance Stress Test’ and are addressed to the NCAs. The report highlights the need to strengthen the supervision of the affected groups and requests the NCAs to review and, where necessary, to challenge capital and risk management strategies of those groups. Furthermore, it states that NCAs should require groups to identify the range of possible management actions, assess whether these actions are realistic and consider potential second-round effects.

In the report, EIOPA also requests NCAs to check the ad-

equacy and flexibility of systems and risk models used by groups for stress testing, and states that for future stress tests NCAs should ensure sufficient resources. EIOPA also calls on NCAs to enhance cooperation and information sharing with relevant authorities, such as the ECB Single Supervisory Mechanism and/or other national supervisory authorities of affected insurers that are part of a financial conglomerate.

Gabriel Bernardino, chairman of EIOPA, said: “The objective of these recommendations is to identify a set of supervisory actions deemed necessary to address risks and vulnerabilities, and to strengthen the ongoing supervision of the relevant insurance groups with the aim of ensuring market stability. EIOPA will monitor implementation of the recommendations by the NCAs.” ■

Source: Commercial Risk Website  
29 April 2019



• ***Growing demand for global cyber insurance programmes to counter cross-border threat***

***By Stuart Collins on June 4, 2019***

Multinational cyber insurance programmes are in their infancy, but interest is growing and longer term they should help companies manage an increasingly global threat.

Corporations are increasingly exposed to cross-border cyber risks through extended supply chains, the growing importance of third-party vendors and mounting international data protection and privacy laws, according to a new whitepaper by Chubb.

This will increasingly require risk and insurance managers to engage with different parts of the business and external experts, and potentially develop more comprehensive global programmes.

Global programmes for cyber risk are still in their infancy, but demand is growing and insurers are looking to develop solutions, Jared Concannon, major accounts segment leader at Chubb told CRE this week at Airmic's conference. Currently, some companies buy global cyber policies, but true global programmes for cyber risk require local policies and servicing, including breach response, he explained.

"As cyber risks evolve and do not discriminate among national borders, the value of local cyber policies with commensurate claims and response services cannot be un-

derestimated," Chubb says in its whitepaper.

"Local policies tailored to local regulations and terms and conditions consistent with locally acceptable customs and practices, are prudent for effective local coverage... A broad global umbrella master policy providing drop-down coverage to fill gaps for differences in conditions and local limits brings efficiency in pricing and needed capacity," it adds.

Demand for global cyber programmes is increasing, according to Karen Gorman, head of global services and solutions GB at Willis Towers Watson. Limited cyber programmes covering key markets like the US and Europe are possible, but insurers are now looking to build out underwriting and servicing capabilities in local markets, she said.

According to Chubb, cyber threats are diverse and ever-changing as global organisations become increasingly reliant on technology and data. At the same time, multinational organisations are increasingly exposed to cyber-related regulation, including sector-specific cybersecurity rules and increased data protection laws.

In addition to the EU's stringent General Data Protection Regulations (GDPR), Canada





Karen Gorman

and Australia are bolstering privacy rules and have recently introduced mandatory data breach regimes. California is also introducing tougher privacy rules, mirroring aspects of the GDPR.

In some cases, such as with the GDPR, these laws have extra-territorial reach, creating exposures for organisations in markets where they may not have physical operations. National data protection laws also typically restrict the transfer of data overseas, while a growing number of bilateral agreements govern such practices.

“A multinational company’s cyber preparedness extends beyond ensuring its IT systems are secure and robust or guarding against the vulnerabilities of third-party vendors or supply chain risks. A global company must also be aware of the relevant legislative requirements for data protection in the countries they operate and understand their main obligations,” Chubb says in its whitepaper.

“Risk managers and data protection officers of global companies need to ensure that policies are in place, data protection impact assessments are carried out and training is provided to staff so that the le-

gal requirements are properly understood,” it adds.

Staying ahead of the “evolution curve” in cyber liability will be challenging for multinational companies, continues Chubb. It is vital that global organisations can access a multidisciplinary team of experts to analyse the evolving threat landscape and regulatory regimes, it adds in its whitepaper. Companies also need help to understand the evolving scrutiny of a multinational company’s data privacy standards, the insurer says.

According to Chubb, it is “imperative” that risk managers maintain engagement with key stakeholders throughout a business, to map out future cyber-related exposures their organisation may face.

“The difficulty in keeping pace with changes in the technologies a business uses, and the various global regulations that govern them, highlights the value of consulting with a broad spectrum of internal and external experts who can counsel and direct how to structure a robust and flexible risk transfer multinational cyber insurance programme,” the insurer adds in its whitepaper. ■

Source: Commercial Risk Online - 4 June 2019



• **Marine cyber risk secondary to environmental focus**



**Maritime sector and insurance technology experts converged on Windward's inaugural Sea: The Future 2019 conference**

Maritime sector businesses are focused on reducing emissions to meet tough new regulatory requirements, meaning that their cyber risk worries are not anywhere near top priority, panelists told a maritime technology event held in London today.

That was the buzz from Windward's "Sea: The Future" conference, held in London's Trinity House.

Windward is a technology services firm using satellite and other data together with artificial intelligence to spot patterns in shipping, detecting risky behaviour for insurers, and illegal activities for government and military clients.

The firm was set up with backing from retired US general David Petraeus, while former BP CEO Lord John Brown joined its board last year, and headlined the Trinity House event.

Speakers at the conference

pointed to new and tougher emissions targets for shipping firms to reduce their carbon footprint set last year by the UN's International Maritime Organization (IMO).

"The last thing on your mind is cyber, I'm afraid," said Harry Theochari, Maritime UK chairman and head of transport law at Norton Rose Fulbright.

"The environment will continue to take centre stage because the IMO is very focused on it," he said,

The IMO has however put "high-level" cyber requirements in place for Safety Management Systems (SMS) that will be implemented by 2021 into the UN body's Safety of Life at Sea (Solus) requirements.

"It's high level and pretty convoluted," Theochari said, noting that other bodies such as the International Chamber of Shipping and various governmental and industry stakeholder groups have been working to provide more detailed guidance.

"By January 2021 SOLAS is





Harry Theochari

making it absolutely mandatory for your SMS systems to be fully cyber compliant,” said Theochari.

**Collateral damage**

The shipping sector, Maersk in particular, was badly affected by the June 2017 Russian state-sponsored Not Petya malware attack, masquerading as ransomware but designed to wipe systems and cause maximum disruption.

That attack was targeted at Ukrainian IP addresses but the shipping sector’s global characteristics meant it was “collateral damage”, said Robert Hannigan, executive chairman, Bluevoyant Europe, speaking on the same cyber risk panel.

“Maritime is subject to the same threats and actors as other sectors,” he said, noting that shipping’s relationship with the energy sector made it subject to “particular leverage” in matters of government-sponsored hybrid warfare, such as state-sponsored cyber attacks.

However, the focus on high profile attacks, such as Russia’s attacks on Ukraine, on Estonia’s banking infrastructure in 2007, and on the US electoral system in 2016, leave the higher frequency lower impact attacks relatively neglected, Hannigan emphasised.

“We focus too much on the low risk high impact attacks [such as NotPetya], for which we need to rely on

governments to defend us,” said Hannigan.

“More focus is needed on the high risk, low impact almost daily cyber attacks on ports and shipping,” he added.

For major cyber attacks, the sector will remain heavily reliant on government, law enforcement, intelligence agencies, and specialist cyber experts in the private market, noted Line Dahl, chief customer officer at marine insurer Gard.

“We don’t have the confidence to save the world alone. We’re pretty dependent on working with the cyber experts,” she said.

Too many cyber attacks are being claimed under traditional policies, even when companies have cyber coverage in place, suggested Itai Sela, CEO of Naval Dome.

He suggested insurers need to demand more information when underwriting shipping businesses about the number of prior claims made for cyber attacks, under the guise of whatever policy.

Doubts about cyber insurance exclusions persist, and have been furthered by recent legal cases, Hannigan emphasised.

Insurers are tightening up their terms and conditions, putting exclusions into place which mean insured firms need to be seen to be taking the right steps to mitigate cyber risks.

“Not doing the right thing is



Robert Hannigan

becoming a cyber exclusion,” Hannigan said, pointing to the importance installing the latest patches to update software in use throughout large businesses.

### Technology v insurance

The insurance industry is prepared to accept that risk prevention technology will nudge insurance out of areas of marine risk that are currently insured, according to Tom Hutton, managing partner at XL Innovate.

Hutton said insurance technology’s rise had been remarkable in recent years, with a “huge opportunity” for insurtech firms and their backers to address risks “related to everything we do linked to the wider economy”.

Preventative risk technology, including predictive analytics, would lead to some currently-insured risks, not being underwritten in future, while providing other opportunities that insurers do not already underwrite, Hutton explained.

“Insurtech will lead to a number of risks not being insured in the future that were insured in the past,” said Hutton.

In essence, insurance innovation may end up in shipping companies buying less insurance.

“Absolutely, and that’s okay,” he said. “We should not just represent a function of protecting the status quo, but of making it better for everybody.”

Despite many successful start-ups, he suggested the needed shakeup of the insurance distribution model has yet to happen.

He compared the situation to that faced a decade ago by airlines worried about online pricing sites affecting their e-commerce business models, noting that airlines have responded effectively and, for the most part, not gone out of business.

For marine insurers, he suggested another innovation was sorely needed: the ability to better track the insured contents of shipping containers as they cross the world’s oceans.

“The insurance industry would dearly love to know where a package is on a container ship somewhere in the world,” Hutton said.

Transmission technology that might be used to keep track of cargo gets disrupted by metal containers, he noted.

“That is a big problem today. Something like 1,400 containers are lost at sea each year. That’s a huge opportunity to solve,” Hutton added. ■



Line Dahl

Global Reinsurance - 22 May 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



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



# Africa News



## Fitch Ratings

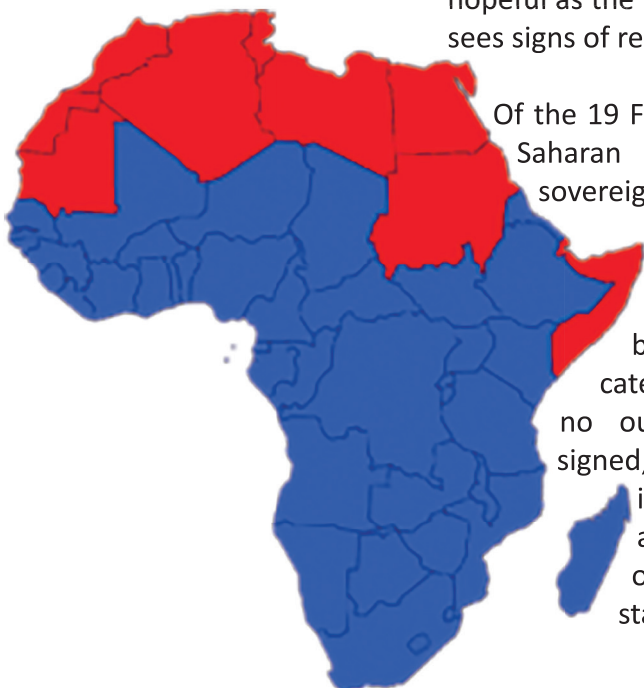
### • Fitch Ratings more optimistic about African fortunes

Lesotho, Namibia and Zambia have been given negative outlooks by Fitch ratings but overall, the outlook for the African continent is more hopeful as the ratings agency sees signs of recovery.

Fitch said that while the number of negative outlooks is still high, some progress on fiscal and external adjustment has been made and median debt/GDP is expected to stabilise.

“This was reflected in the decision to revise the outlooks on Kenya’s and Angola’s ratings to stable from negative in February and April 2018, respectively. However, the outlook on Lesotho’s B+ IDR was revised to negative from stable in August 2018,” said Fitch.

Fitch expects SSA’s recovery to continue in 2019, with the three largest economies in the region experiencing moderate growth and several oth-



Of the 19 Fitch-rated Sub Saharan Africa (SSA) sovereigns, three carry a negative outlook, two have a rating below the B category where no outlook is assigned, one is on positive outlook, and all the others have a stable outlook.



er oil exporters seeing growth accelerate.

“Some strong performers, including Ethiopia and Côte d’Ivoire, will see growth slow but we forecast median growth of 4.5% in 2019, up from 3.7% in 2018,” Fitch added.

Higher commodity prices have reduced exporters’ external imbalances, but current account deficits will widen in 2019 and 2020, partly due to high infrastructure investments, warned Fitch.

“Angola and Nigeria have seen their foreign exchange liquidity improve following adjustments to their FX regimes, but a number of SSA countries will experience currency volatility, in line with emerging markets more broadly.

“Cameroon and Gabon are on International Monetary Fund (IMF) programmes, which have aided their external positions, but it is still uncertain whether the Republic of Congo and Zambia will reach agreements with the fund,” it concluded.

IMF programmes and a rise in oil prices will contribute to stabilising debt/GDP in many SSA sovereigns. Low revenue mobilisation will keep debt/revenue ratios high. A number of SSA sovereigns have tapped, or are planning to tap, Eurobond markets in 2019 but Eurobond financing is likely to become more costly and difficult as risk appetite has declined, suggested Fitch. ■

**Commercial Risk Africa**

Source: Commercial Risk Website  
30 April 2019



## • 2017 ranking of the African reinsurance companies according to turnover

In thousands USD

Ranking		Company	Country	2013	2014	2015	2016	2017	Evolution (%)	
2017	2016								2016-2017	2013-2017
1	1	Africa Re	Nigeria	670458	717525	689291	642024	746829	+16.32	+11.39
2	2	Munich Reinsurance of Africa	South Africa	470672	485571	388455	556433	681638	+22.50	+44.82
3	3	Compagnie Centrale de Réassurance	Algeria	261454	255169	237674	236528	256282	+8.35	-1.98
4	5	Hannover Life Reinsurance Africa	South Africa	206099	184241	156588	188161	215836	+14.71	+4.72
5	4	Société Centrale de Réassurance	Morocco	264052	299900	255543	235500	215580	-8.46	-18.36
6	9	RGA Reinsurance Co. of South Africa	South Africa	118372	125454	98047	169618	212290	+25.16	+79.34
7	7	Hannover Reinsurance Africa	South Africa	254058	265316	155587	179153	204582	+14.19	-19.47
8	10	African Re Corporation (ARCSA)	South Africa	-	206890	160354	157911	203500	+28.87	-
9	8	General Reinsurance Africa	South Africa	193141	182398	144846	173209	194145	+12.09	+0.52
10	6	Swiss Re Life & Health Africa <sup>(1)</sup>	South Africa	137417	138000	122500	180100	ND	ND	ND
11	12	Zep Re (PTA Re)	Kenya	100181	125437	138756	128698	152132	+18.21	+51.86
12	11	Kenya Re	Kenya	113330	129931	129924	131664	144952	+10.09	+27.90
13	16	GIC Re South Africa <sup>(2)</sup>	South Africa	1552	12900	22069	53074	138614	+161.17	+8831.31
14	13	Scor Africa	South Africa	83118	81395	72350	78792	124872	+58.48	+50.23
15	15	CICA-Re	Togo	48030	50425	55295	69821	84629	+21.21	+76.20
16	14	Continental Re	Nigeria	99403	83648	100052	73940	83382	+12.77	-16,12
17	17	Waica Re	Sierra Leone	15922	24124	33542	49201	62119	+26.26	+290.15
18	18	Tunis Re	Tunisia	43884	48046	49499	45668	48984	+7.26	+11.62
19	21	Ghana Re	Ghana	36323	32417	32997	33380	42518	+27.38	+17.06
20	22	East Africa Re	Kenya	33105	39058	36857	33084	40344	+21.94	+21.87
21	19	Africa Retakaful	Egypt	-	-	41566	45295	38960	-13.99	-
22	20	Tan Re	Tanzania	40274	43253	34527	35305	34734	-1.62	-13.76
23	24	Aveni Re	Côte d'Ivoire	25566	27136	25604	26090	29951	+14.80	+17.15
24	26	National Re	Sudan	26355	11200	17800	24285	29073	+19.72	+10.31
25	25	NCA Re	Côte d'Ivoire	11744	20314	24240	25800	28338	+9.84	+141.30
26	23	Sen Re	Senegal	28358	28383	29816	26444	25457	-3.73	-10.23
27	31	Namibre <sup>(2)</sup>	Namibia	16050	14786	14164	14007	23638	+68.76	+47.28
28		Ethiopian Reinsurance <sup>(3)</sup>	Ethiopia	-	-	-	-	22538	-	-
29	27	SCG Ré	Gabon	18143	20541	26189	18194	22445	+23.36	+23.71
30	33	Globus Re	Burkina Faso	16457	11153	12527	13699	20938	+52.84	+27.23
31	28	ZB Reinsurance	Zimbabwe	20551	20721	20885	19130	19099	-0.16	-7.07
32	30	FBC Re	Zimbabwe	15227	15662	17799	14059	18741	+33.30	+23.08
33	29	First Mutual Reinsurance	Zimbabwe	20048	19790	19806	17196	16569	-3.65	-17.35
34	32	Grand Reinsurance	Zimbabwe	5728	8114	10333	13841	15267	+10.30	+166.53
35	34	Tropical Re	Zimbabwe	11128	13869	14144	13548	15208	+12.25	+36.66
36	35	Zep Re	Zimbabwe	-	9833	9407	10903	12917	+18.47	-
37	37	Mamda Ré	Morocco	-	-	-	9493	12182	+28.33	-
38	39	GN Reinsurance	Ghana	-	-	3380	7025	9319	+32.65	-
39	36	Baobab Reinsurance	Zimbabwe	15207	8410	8791	9291	9176	-1.24	-39.66
40	38	Uganda Re	Uganda	255	5459	6545	7122	7992	+12.22	+3034.12
46	41	Prima Re	Zambia	4631	4790	3032	3711	3984	+7.36	-13.97
41	40	Baobab Life & Health	Zimbabwe	-	5483	4152	4170	3754	-9.98	-
42	43	Nigeria Re <sup>(1)</sup>	Nigeria	2990	4350	3552	2365	ND	ND	ND
43	42	First Mutual Reinsurance (Life & Health)	Zimbabwe	2000	4725	2984	2515	2160	-14.12	8
44	44	Colonnade Re	Zimbabwe	5005	3777	2661	1963	880	-55.17	-82.42
45	45	FBC Re	Zimbabwe	-	-	ND	693	665	-4.04	-

<sup>(1)</sup> Figures 2017 not available<sup>(2)</sup> Fiscal year ending March 31<sup>st</sup><sup>(3)</sup> Established in July 2016



# ALGERIA

## • Algerian insurance market: results 2018

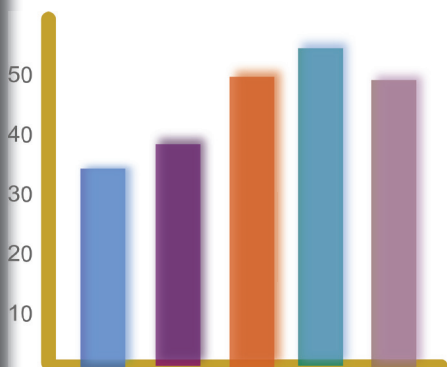
According to the national insurance council (CNA) the Algerian insurance market has recorded a total turnover (direct business and acceptances included) of 142.6 billion DZD (1.193 billion USD) for 2018, thus increasing by 2.2% over one year.

The non-life activity recorded 88.4% of premiums reaching 126 billion DZD (1.1 billion USD), and increasing by 3.2% compared to 2017. In contrast, the life insurance activity declined by 10.5% at 12.2 billion DZD (102 million USD).

The motor class of business remains the most profitable notably after recording 68.9 billion DZD (576 million USD) in premiums in 2018. This activity totals up 48.3% of the total premiums on the market.

The fire and miscellaneous accidents are ranked second after the motor activity with a turnover of 46.6 billion DZD (390 million USD) which represents 32.6% market share. In addition, the «natural disasters» premiums remarkably rose by 66.5%. ■

Sources: Atlas Magazine – 17 April 2019



# ANGOLA

## • Creation of a national reinsurer in Angola



AGÊNCIA ANGOLANA DE REGULAÇÃO E SUPERVISÃO DE SEGUROS

The Angolan Agency for Regulation and Supervision of Insurance has announced the forthcoming establishment of a national reinsurance company, named AngoRe. Being finalised, the project should be presented to potential shareholders in three months.

The roundtable will include the Angolan State as well as local and foreign private investors. AngoRe should increase the retention capacity of the local market.

The number of licensed insurance companies in Angola continues to increase but at a much slower pace than previously. In 2016, six new companies were granted licences and in 2017 and 2018, only one company was licensed in each year.

There are 26 insurance companies licensed in Angola. The two state-owned companies are licensed as composite insurers, although AAA is under-

stood by many market sources to have ceased trading in all lines. The remaining companies are privately owned and all have both life and non-life licences.

Angolan insurance business regulated by the Angolan Agency for Regulation and Supervision of Insurance (Agencia Angolana de Regulacao e Supervisao de Seguros - AR-SEG)

Regarding the market performance in 2017 according to preliminary data, Angolan non-life market premium (including PA and healthcare) increased by 7.6% and was estimated to have reached AOA 108.06bn (USD 651.29mn), of which 43.47% was PA and healthcare. In local currency terms the non-life market (including PA and healthcare) grew in 2014, 2015 and 2017 but contracted in 2016 by almost 10%. Figures for the market.

In local currency terms, mark a contraction in the market in real terms between 2014 and 2017 due to significant economic difficulties, devaluation of the currency, and a strong upsurge in inflation. In USD terms, the non-life market (including PA and healthcare) generated USD 1,026.62mn in premiums in 2014 which contracted to just USD 651.29mn in 2017. ■

Sources: Atlas Magazine & AXCO

# CAMEROON

• *Wafa assurance acquires a life and a non-life insurer in Cameroon*



Wafa Assurance has become a majority shareholder in Pro Assur SA and Pro Assur Vie.



تأمين الوفاء  
Wafa Assurance

Pursuant to the terms of the rapprochement agreement contracted by both parties, Wafa proceeds with a capital increase of a Pro Assur followed by the acquisition of 65% of shares and voting rights in the non-life Cameroonian insurer.

The Moroccan insurer acquires a controlling interest of 89.4% of shares and voting rights in Pro Assur Vie.

These operations are yet to be approved by the Moroccan and Cameroonian authorities. ■

Sources: Atlas Magazine – 26 April 2019





**MISR LIFE INSURANCE**  
TOMORROW STARTS TODAY

**YOUR CONVENIENCE IS OUR GOAL**

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

GET THE APP



[misr\\_life\\_ins](#)



[misrlifeinsurance](#)

[www.misrlife.com](http://www.misrlife.com) / call 19446

مصر القابضة للتأمين  
MISR INSURANCE HOLDING COMPANY



# Egypt

- **Insurers post higher premium income but lower net gains in FY2018**

The Egyptian insurance market posted total premiums of around EGP30bn (\$1.76bn) for the fiscal year ended 30 June 2018 (FY2018), a growth rate of around 23.4% compared to the EGP24bn chalked up for FY2017, according to the latest annual report of the Financial Regulatory Authority.

Insurance companies paid total compensation of about EGP15.4bn in FY2018, 19.4% higher than in FY2017, reported Youm7 citing the annual report.

Mr Reda Abdel Moaty, FRA deputy chairman, said that net profits of the insurance sector in Egypt for FY2018 fell by 23% to around EGP3.7bn. He pointed out that despite the decline in FY2018, the results had improved over the last four years. Net gains of the industry stood at EGP2bn for FY2014. This increasing trend has resulted in more investments entering the Egyptian insurance market through the establishment of new companies.

Shareholders' equity in insurance companies reached EGP38bn at 30 June 2018, 23.3% higher than a year ago.

The number of insurance companies operating in Egypt stood at 37 at 30 June 2018.

The FRA annual report also says that 60% of insurance companies in Egypt were issuing policies in electronic form by June 2018. The regulator is encouraging the insurance sector to turn to technology in the issuance and distribution of standard insurance policies which do not require complicated subscription steps. The types of insurance policies which the FRA allows to be issued electronically include personal accident insurance, travel insurance, short term life insurance and compulsory motor third party liability insurance. ■

Source: Middle East Insurance Review | 23 May 2019

- **Microfinance activity records 6 bn pounds in Q1 2019**

Egypt's microfinance activity balance has increased over the first (Q1) of 2019 to register 6 billion Egyptian Pounds for around 960.06 beneficiaries compared to 3.3 billion pounds in the same period of 2018.

Thus the microfinance activity balance is capturing 48 percent of the financing activity, according to The Financial Regulatory Authority (FRA).

There are nine companies working in the micro-finance activity in Egypt namely Reefy, Tanmeyah, Tasaheel, Amaan, Sanda, Tamweely, Fawry, Al Oula and Vitas.



Reda Abdel Moaty



In the second place came the category “A” associations recording total volume of funds of 5.3 billion Egyptian pounds, accounting for 41.9% of the total finances, compared to 4 billion pounds at the end of the first quarter of 2018, according to a report issued by EFSA.

The category “B” associations recorded funds of 643.1 million pounds at the end of the first quarter of 2019, accounting for 5.08% of the total value of finance, compared to 572.6 million pounds at the end of March 2018.

The category “C” associations registered 627.7 million pounds funds by the end of March 2019, compared to 505 million pounds by the end of March 2018.

The micro insurance is a key foundation to support micro-finance, providing insurance protection to these funds in addition to covering the projects that have received them.

■ Source: Amwal Alghad (<https://en.amwalalghad.com>) 19 May 2019

### • **Compulsory motor insurance tariffs for electric and hybrid cars in Egypt**

The Financial Regulatory Authority (FRA) has released the compulsory motor insurance tariffs for electric and hybrid cars in Egypt.

The insurance premium for a passenger cars is 12 EGP (0.71 USD) per month and 120 EGP (7.12 USD) per year. For commercial vehicles and trailers, an additional premium is set according to the weight.

The premium for cars with provisional license plates is EGP 120 (7.11 USD) per month, 150 EGP (8.89 USD) for two months and 200 EGP (11.86 USD) for three months.

For taxis, buses, and tourist cars boarding up to seven people, compulsory insurance is charged to the number of passengers.

For electric or hybrid motorcycles, the insurance costs EGP 10 (0.59 USD) per month or 100 EGP (5.93 USD) per year. The premium is higher for a vehicle with a cylinder capacity exceeding 500 cc, a quad bike or a tricycle. ■

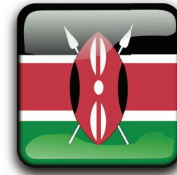
Source: Atlas Magazine – 29 May 2019





# KENYA

• *West Africa reinsurer WAICA Re expands to Kenya*



West African reinsurer WAICA Re has launched new operations in Kenya in an effort to capitalize on the growing insurance market in East and Central Africa, according to reports from Standard Digital.

WAICA Re Kenya is set to provide reinsurance for all general classes across the region.

The unit has a capital outlay of KES 1 billion (USD \$9.9 million) and is expected to grow its annual income to KES 1.5 billion (USD \$14.9 million) over the next three years.

“Kenya’s insurance sector has a lot of growth potential and the country’s favourable policy framework has created a friendly environment for investment and growth,” Charles Etemesi, CEO of WAICA Re Kenya, said at the launch in Nairobi this week.

He explained that the business would rely on technology and the capital position of its parent company to grow its market share in the highly competitive sector.

“We are going to deploy cutting-edge technology, especially in document management systems and relevant finance and underwriting software to ensure that we run an efficient business that will add value to our clients,” Standard Digital quoted Etemesi as saying.

The publication noted that insurance penetration in Kenya has traditionally been very low, with recent data putting it at just 2.8% of the population, compared to 3.5% in sub-Saharan Africa. ■



Charles Etemesi

Source: Reinsurance News (ReinsuranceNe.ws) | 28 March 2019





# MOROCCO

## • Agricultural insurer signs pact to provide poultry insurance



The Moroccan Agricultural Mutual Insurance Company (Mamda) and the Interprofessional Federation of the Poultry Sector (FISA) have signed an agreement for the distribution of insurance products for the poultry sector.

This is the first time that Mamda has launched products for poultry farmers.

The insurance plan offers payouts to the farmers if their poultry stock contracts one of three types of diseases deemed legally contagious, namely, Highly Pathogenic Avian Influenza (HPAI), Newcastle Disease (ND) and Salmonella Pulorum Galinarum (SPG).

Mamda will also offer to all members and their employees a range of insurance products tailored to their activities. Thus, the newly designed poultry insurance is part of a

basic scheme that includes comprehensive automobile, industrial accident and occupational diseases, third party liability as well as fire-explosion or industrial multi-risk insurance.

The package can be enriched by additional covers such as individual accident, illness, retirement, death and disability and the transportation of goods.

In coordination with FISA, Mamda will conduct awareness campaigns for the beneficiaries of the agreement, to raise awareness about the scope of the insurance products offered and their impact on the daily activity of operators in the sector.

Apart from FISA members, those who are part of professional organisations in the poultry industry can subscribe to the insurance scheme. These organisations include the Association of Compound Feed Manufacturers (AFAC), the National Association of Moroccan Hatcheries (ANAM), the National Association of Meat Producers, the National Association of Egg Producers (ANPO) and the National Association of Poultry Slaughterhouses (ANAVI). ■



Source: Middle East Insurance Review | 19 May 2019

# NIGERIA

## • NAICOM raises capital base of insurance companies by over 300%

The National Insurance Commission (NAICOM) has increased the minimum paid-up capital of insurance companies in Nigeria by over 300 percent. This was contained in a circular (released 20 May 2019) by the Commission and signed by Pius Agboola, the Director, Policy and Regulation Directorate, for the Commissioner of Insurance.

The circular with No. NAICOM/DPR/CIR/25/2019, titled “Minimum paid-up share capital for insurance and reinsurance companies” the minimum paid-up share capital requirement of insurance and reinsurance companies in Nigeria is hereby reviewed as follows:

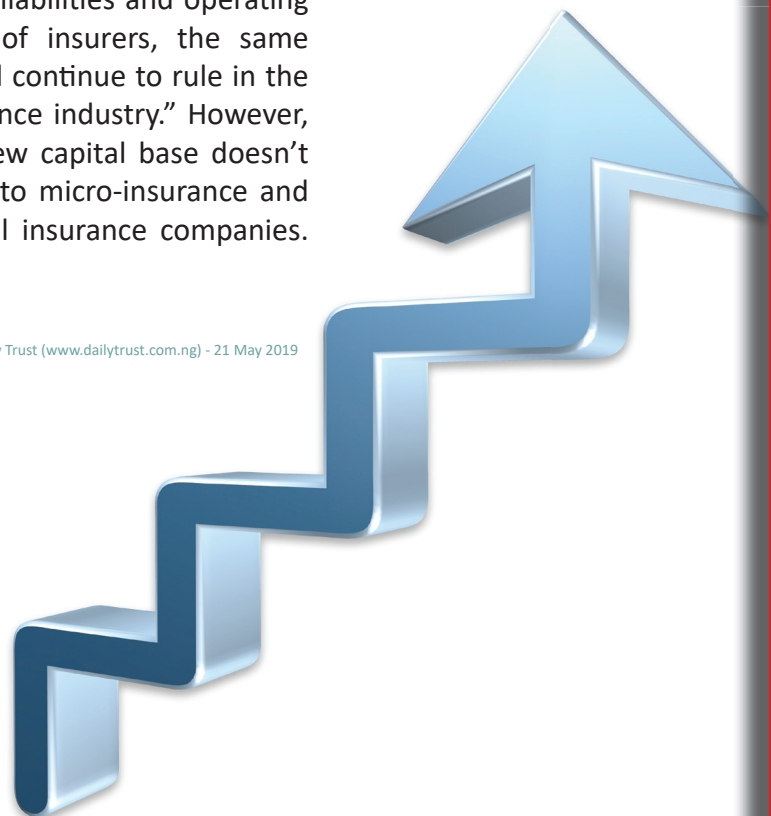
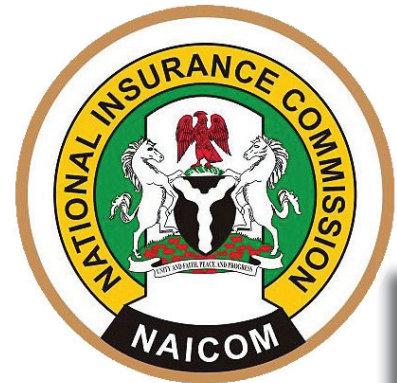
- In the new capital base, life insurance companies will now have a minimum paid-up capital of N8bn from its previous N2bn.
- General Insurance companies will now have to re-capitalize to N10bn from N3bn
- Composite Insurance companies will now need N18bn to underwrite businesses from the previous N5bn minimum capital.
- The new capital base requirement also affected reinsurance companies who will now have to raise their minimum paid-up capital from N10bn to

N20bn if they must remain in business.

The circular said that “the new minimum paid-up share capital requirements shall take effect from the commencement date of this circular for new applications while existing insurance and reinsurance companies shall be required to fully comply not later than June 30, 2020.”

In reviewing the paid-up capital, the Commission noted that “in 2005/7, the insurance industry witnessed its last recapitalisation and despite the astronomical increase in value of insured assets, consequent exposure to higher level of insured liabilities and operating costs of insurers, the same capital continue to rule in the insurance industry.” However, the new capital base doesn’t apply to micro-insurance and Takaful insurance companies.

Source: Daily Trust ([www.dailytrust.com.ng](http://www.dailytrust.com.ng)) - 21 May 2019





Everyone needs a risk solution partner...

... we can be yours.

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](http://www.malaysian-re.com.my)



# Asian News



## ASIA PACIFIC

### • Risk Based Capital: A Comparative Review

#### Cambodia



Insurance companies and intermediaries shall maintain a deposit to the National Treasury.

Insurance Company: 10 per cent of registered capital  
Insurance Broker: US\$50,000  
Insurance Agent and Loss Adjustor: US\$10,000

Insurance companies shall maintain a solvency margin:  
For the first year of operation: 50 per cent of the registered capital; thereafter

- KHR13.3 billion, where net premiums  $\leq$  KHR66.5 billion.
- 20 per cent of total premium, where net premiums are between KHR66.5 billion and KHR332.5 billion.
- KHR66.5 billion plus 10 per cent of insurance surplus

from the previous year where net premium is < KHR332.5 billion.

in each case assessed on the previous year's premiums. Professional liability insurance: US\$500,000 applicable only to insurance brokers.

#### People's Republic of China



Yes.

China formally launched a Solvency II type regime in May 2013 and have fully implemented it since 2016, which includes a three-pillar structure. One of the three pillars is the requirement of capital quantification, which obliges an insurer to identify and quantify categories of risks (such as insurance risks, market risks, credit risks, etc.) and support such risks with a comparable amount of capital.



Categories of risks are open to expansion - for example reputation risk was added in 2014. The regime keeps developing – a phase II update has started in late 2017 and plans to be completed by the end of June 2020.



**Hong Kong**

No, the current framework is a rules-based capital adequacy framework. However, an insurer must maintain an excess of assets over liabilities of not less than a required solvency margin.

**General – the greater of**

- 20 per cent of relevant premium income up to HK\$200 million plus 10 per cent of the amount by which the relevant premium income exceeds HK\$200 million.
- 20 per cent of relevant outstanding claims up to HK\$200 million plus 10 per cent of the amount by which the relevant outstanding claims exceed HK\$200 million.

Subject to a minimum of HK\$10 million (HK\$20 million for certain statutory classes).

**Life – the greater of**

- HK\$2 million.
- Generally 4 per cent of mathematical reserves plus 0.3 per cent of capital at risk.

There are proposals to introduce a risk-based capital framework. The former IA published consultation conclusions in September 2015 on the proposed introduction of a risk-based capital framework in line with core principles

of the International Association of Insurance Supervisors (IAIS). It is proposed that the framework will comprise three pillars (Pillar 1: quantitative requirements; Pillar 2: qualitative requirements; and Pillar 3: disclosure and transparency requirements) and will be introduced on a phased basis; the next step being the development of detailed rules which are tentatively expected to be ready for public consultation in 2020.



**India**

Every insurer and re-insurer shall at all times maintain an excess of value of assets over liabilities of not less than 50

per cent of the amount of minimum capital that such insurer or re-insurer is required to bring.

Available Solvency Margin (ASM) i.e. the value of assets over the value of life insurance liabilities and other liabilities of policyholders’ funds and shareholders’ funds, shall not be less than the higher of (a) 50 per cent of the amount of minimum capital prescribed and (b) 100 per cent of the Required Solvency Margin (RSM).

“Control level of solvency margin” is specified to be a solvency ratio (ASM/RSM) of 150 per cent. Indian insurers are permitted to place reinsurance business with cross border reinsurers (CBRs) not having a physical presence in India and doing reinsurance business with Indian insurance companies, who comply with the eligibility criteria specified by IRDA, which are, inter alia,



maintenance of solvency margin/capital adequacy as stipulated by the home regulator of the CBR.



### Indonesia

Specific risk factors which must be taken into account include credit risk, liquidity risk, market risk, insurance risk and operational risk. **TNB Note:** the above changes are based on OJK Regulation No. 71/POJK.05/2016 on the Financial Soundness of Insurance Companies and Reinsurance Companies which was enacted in late December 2016.



### Japan

The IBA provides for calculation of a solvency margin ratio:

**Solvency margin ratio (per cent):**  
 $(\text{Total amount of solvency margin} \times 100) / (\text{Total amounts of risk} \times 0.5)$

The total amount of risk is calculated using different formulas for life and non-life insurance, taking into account potential volatility or deviations in claims, interest rates, asset valuations, credit risk, business risks, minimum guarantee risk and catastrophe risks.

A solvency margin of

- 200 per cent or more: sound condition, no intervention by the FSA.
- Less than 200 per cent and no less than 100 per cent: the FSA will issue a “business improvement order”.
- Less than 100 per cent and no less than 0 per cent: the FSA will order measures to improve capability to pay claims, e.g. suspension of dividends to shareholders and/or policyholders, change of terms for new

business, or prohibition on directors’ bonuses.

- Less than 0 per cent: the FSA will order partial or total suspension of business.

### Korea, South

Yes, since April 1, 2011.



### Macau

Non-life insurance companies must maintain a solvency ratio determined in accordance with the total amount of gross written premiums of the previous year, as follows



Gross written premiums	Solvency ration
< MOP10 million	MOP5 million
= or > MOP10 million and < MOP20 million	50 per cent of the gross premium amount
= or > MOP20 million	MOP10 million plus 25 of the amount in excess of MOP20 million of gross premiums

Life insurance companies must maintain a solvency ratio determined by a set of formulas that take into account the mathematical reserves of the main technical provisions and the risk based capital.

An insurance company solvency ratio must be composed by tangible unencumbered assets. AMCM publishes a yearly list of assets which are excluded from incorporating the solvency ratio of authorised insurers.

Currently the control measures for failure to maintain the requisite solvency ratios are determined by AMCM as follows –

Solvency Ratio	Regulatory control measures
More than 150%	Life insurance companies must proceed with periodic stress-tests related to their solvency capacity, to identify potential risks and respective consequences.
Between 100% and 150%	Life insurance companies are required to submit a financial recovery plan to AMCM and report the performance periodically.
Between 70% and 100%	AMCM will take necessary supervisory measures to guarantee the rights of the policy holders.
Less than 70%	AMCM will take necessary measures to interfere the operation of the life insurance companies.

**Our foundation**  
goes real deep.

**Total Assets:** US \$ 12 billion

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

**Global Ranking (2015):**

14<sup>th</sup> among Global Reinsurers (A M Best)

18<sup>th</sup> among Global Reinsurers (S & P)

**Ratings:**

**Financial Strength:** A- (Excellent) A M Best Company

**Claims Paying Ability:** "AAA(In)" by CARE



आपत्काले रक्षिष्यामि  
GIC Re

**General Insurance Corporation of India**

Global Reinsurance Solutions

Website: [www.gicofindia.in](http://www.gicofindia.in)

Contact us at [info@gicofindia.com](mailto:info@gicofindia.com)

GICRE/CAPL/06-16/1Q-001



**Malaysia**

Yes, the Risk-Based Capital Framework applies to all insurers, including reinsurers, licensed under the Financial Services Act 2013, for business generated within and (subject to limited exceptions) outside Malaysia. The Framework was first implemented with effect from January 1, 2009.

$CAR = \frac{\text{Total Capital Available}}{\text{Total Capital Required}} \times 100$  per cent.)

Total capital available (TCA) is the aggregate of Tier 1 capital (such as issued and paid-up ordinary shares) and Tier 2 capital (such as cumulative irredeemable preference shares) less deductions from capital (such as goodwill, deferred tax assets and investment in subsidiaries). The total amount of Tier 2 capital must not exceed the amount of Tier 1 capital. Total capital required (TCR) is the aggregate of capital charges for each insurance fund and assets in the shareholders fund/working fund. Capital charges are fixed for credit risk, market risk, insurance liability risk and operational risk or surrender value capital charges.

BNM has set a Supervisory Target Capital Level of 130 per cent.

Each insurer must set its own Individual Target Capital Level to reflect its own risk profile. The Individual Target Capital Level must be higher than the Supervisory Target Capital Level.

**Mongolia**

No. The Solvency Requirement (SR) is determined as below,

subject to the FRC's discretion.

**Ordinary Insurers**

Proper Ratio of Solvency =  $\frac{\text{admitted assets}}{\text{mandatory assets+debts and payments}} \times 100$

If the Proper Ratio of Solvency is < 100 per cent the insurer will be considered insolvent.

**Long Term Insurers**

Proper Ratio of Solvency =  $\frac{\text{admitted assets}}{\text{debts and payments}} \times 100$

The Proper Ratio of Solvency shall be  $\geq 125$  per cent.

If the ratio is between 125 per cent – 100 per cent, the insurer will be presumed to become insolvent.

If the ratio is less than 100 per cent the insurer will be considered insolvent.

Solvency Margin = admitted assets – debts and payments.

The Solvency Margin shall be  $\geq$  the Minimum Solvency Requirement (MSR).

The MSR = actuarial per centage of the reserve fund + valuation per centage of risk of insurance policies.

**Myanmar**

No – capital requirements are based on a solvency margin.

A separate fund for each class of general business and for life assurance must be established.

**Philippines**

Yes. For life and non-life insurers, RBC takes into account credit risk, insurance risk, market risk, operational risk, and catastrophe risk. For

**RISK INSURANCE**

life insurers, RBC additionally takes into account surrender risk. Each insurance company must maintain a minimum RBC ratio of 100 per cent.



**Singapore**

Every licensed insurer shall establish and maintain a separate insurance fund for each class of business carried on by that insurer, and this applies to both Singapore policies as well as offshore policies. A life insurer shall also have separate funds for investment-linked, participating and non-participating policies.

An Insurer must hold capital against its risk exposures, known as Total Risk Requirements (TRR), for each insurance fund and the insurer in aggregate.

TRR is calculated in three components: C1 – insurance risks, C2 – asset portfolio risks, including market and credit risks and C3 – asset concentration risks.



**Sri Lanka**

Currently a solvency margin (risk based capital) model applies to insurance companies whereby every insurance company must maintain

- A capital adequacy ratio (CAR) of a minimum of 120 per cent, (calculated in line with a prescribed formula).
- A total available capital (TAC) of a minimum of LKR500 million (calculated in line with a prescribed formula).



**Taiwan**

Yes. An insurance company

must maintain a ratio of total adjusted net capital to its risk-based capital requirement of at least 200 per cent. The risk-based capital requirement is determined by a formula that takes into account asset risk, insurance risk, interest rate risk and business risk.



**Thailand**

Yes – Eligible Capital/Risk Capital Requirement x 100 per cent = risk based capital.

Eligible Capital is equity, share premium, retained profits, issued price of preference shares, etc. less certain deductions. Assets are valued at market value with adjustments.

Risk Capital Requirement is capital charges for insurance risk, market risk, credit risk and concentration risk.

Solvency margin: minimum capital requirement of 140 per cent of risk based capital.



**Vietnam**

No – capital based.

The minimum solvency margin of a general insurer or a local branch of a foreign insurer is the greater of either (a) 25 per cent of the total premiums actually retained or (b) 12.5 per cent of the total primary insurance premiums plus re-insurance premiums, at the time of determination of the solvency margin.

The minimum solvency margin of a life or health insurer is

- 1.5 per cent of the insurance reserves plus 0.3 per cent of the sums insured which carry risks for unit-linked insurance policies.

- 4 per cent of insurance reserves plus 0.3 per cent of the sums insured which carry risks, for universal life insurance and pension insurance policies.
- 4 per cent of the insurance reserves plus 0.1 per cent of the sums insured which carry risks, for other life insurance policies and health policies with a term of 5 years or less; and 4 per cent of the insurance reserves plus 0.3 per cent of the sums insured which carry risks, for other life insurance policies and health policies with term of over five years.

The minimum solvency margin of a reinsurer is the total of those applicable to a general insurer and a life or health insurer.

Insurers, brokers, and branches of foreign insurers must also establish a mandatory reserve fund to ensure their solvency. The annual contribution is 5 per cent of after-tax profits up to a maximum of 10 per cent of charter capital of an insurer or a broker, or allocated capital of a foreign general insurer’s branch.

**Australia** 

An insurer must have capital in excess of its Prudential Capital Requirement (PCR). The PCR is the prescribed capital amount plus any supervisory adjustments made by APRA in respect of each insurer. The prescribed capital amount can be calculated using either APRA’s “Standard Method” or an internal model approved by APRA. The Standard Method

calculates the capital amount based on insurance risk, asset risk, asset concentration risk and operational risk.

Life insurers additionally have a separate solvency requirement. Under the solvency requirements, a life insurer’s statutory fund must have a capital base that exceeds 90 per cent of the fund’s prescribed capital amount.



**New Zealand**



Solvency Margin is the excess of Actual Solvency Capital (ASC) over Minimum Solvency Capital (MSC), expressed as a dollar amount.

ASC is the total of capital less deductions from capital.

MSC = Total Solvency Requirement (TSR) less, in the case of life insurance, the aggregate of Policy Liabilities and Other Liabilities.

TSR = sum of capital charges for certain key business metrics including: insurance risk, catastrophe and asset risks (including credit, equity and property risk, foreign currency and interest rate risk, asset concentration risk and reinsurance recovery risk).

Policy Liabilities are valued on a best estimate basis and Other Liabilities are valued under NZ GAAP.

Any likely breach over the next three years must be reported.

■

Source:  
2019: Insurance Regulation in Asia Pacific: Ten things to know about 20 countries  
Norton Rose Fulbright, January 2019





• **Emerging Asia drives global premium outlook**

Munich Re expects global primary insurance premium volume to reach almost €7.5trn by 2030. The increase during the next 12 years should be in excess of €3trn, the reinsurer says in its newly published Insurance Market Outlook. A full third of the amount will come from China, and more than €600bn from the US.

The global insurance market will grow by €370bn to almost €4.7trn by 2020, according to Munich Re. Average growth of 4.2% pa (in real terms, inflation adjusted, 2.7%) corresponds with the insurance industry growing at a slower rate than the economy as a whole (expected GDP growth until 2020: nominal 4.4% pa, real 2.9% pa).

After strong growth in premiums in 2018, in part due to high losses from natural disasters, Munich Re expects solid increases in premiums in the largest market, the US, to continue at the average rate of the past few years.

“Emerging nations in Asia are likely to remain the growth frontrunners, despite the economic slowdown in China,” Munich Re says. “In western Europe, we anticipate continued modest growth, while increases in Latin America are being driven by the economic recovery in Brazil.”

The top three markets in emerging Asia are pushing exceptional long-term growth in the region. “Whereas real

growth rates for P&C insurance premiums in industrialised countries are between 1.5% and 2% pa, we expect annual growth of between 3% and 4% in emerging markets,” Munich Re says. “Emerging Asia is the exception. In light of the continuous high growth rates in India, Indonesia and especially China, the region will achieve average real growth rates of as much as 7% pa in the long term.”

Despite only modest growth rates in the US up to 2030, it will probably remain the world’s largest insurance market because of its high premium volume. However, China – currently in second place – will gain significantly during the next few years.

Japan, the UK and France will remain in third, fourth and fifth places respectively. ■

Source: Commercial Risk Website  
3 May 2019

• **Moody’s report examines Japan and China’s solvency regimes**



Japan and China, the two largest insurance markets in Asia, have taken different approaches to solvency regimes that reflect the unique fundamentals of their markets, according to a new report from Moody’s Investors Service. The report

compares China's insurance solvency regime and Japan's solvency practice to the European Solvency II regime.

It notes that China's Risk Oriented Solvency System (C-ROSS) is structured in a similar way to Solvency II but differs on certain disclosure standards and capital charges, while Japan's economic solvency ratio (ESR) practices make frequent references to Solvency II and the Global Insurance Capital Standard (ICS), but implementation remains voluntary.

"China's Risk Oriented Solvency System (C-ROSS) is structured in a similar manner as Solvency II, but was also designed to better fit the development stage of the country's insurance industry and the still-developing state of its financial markets. The upcoming C-ROSS Phase II, however, will introduce more stringent capital requirements and improve transparency on asset risks," said Frank Yuen, a Moody's vice-president and senior analyst.

C-ROSS is based on a three-pillar regulatory framework, like Solvency II, but it follows China GAAP accounting as the basis for valuation.

"This leaves the insurers' solvency ratios less sensitive to short-term capital market volatility and means they reflect more the insurers' long-term holding periods for investments," states the report. "In addition, the different ap-

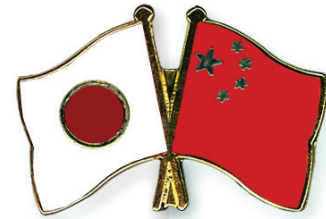
proach taken by C-ROSS on disclosure standards and capital charges results in lower capital requirements for equity and credit risks and also lowers the comparability with Solvency II."

Moody's adds that C-ROSS, which adopts regulator-led supervisory tools more extensively, is also helping to promote and unify risk management best practices in the Chinese insurance industry.

"By comparison, Japan's [ESR] practices are driven largely by enterprise risk management. They are broadly similar to Solvency II practices in terms of quantitative approach, in that both practices are in line with global trends in economic capital modelling," said Soichiro Makimoto, a Moody's vice-president and senior analyst. "Japanese ESR practices make frequent references to Solvency II and the risk-based ICS."

In Japan, since ESR practices are driven by insurers on a voluntary basis, there is wide variability among insurers regarding their disclosure of economic metrics, the report reveals. "While insurers in Japan compute ESRs according to their own discretion, they could raise credibility by improving the transparency and explanation of the process. Such a development would also facilitate appropriate understanding and oversight by external stakeholders and strengthen market discipline," the Moody's report states. ■

Source: Commercial Risk Website  
26 April 2019



Frank Yuen



Soichiro Makimoto

# Your role is Insurance Ours is your Protection

Reinsurer since 1960



**Gross Capacity**  
**US\$ 34 000 000**

**E-mail:** [poolfair@scrmaroc.com](mailto:poolfair@scrmaroc.com)  
**Web:** [www.poolfair.ma](http://www.poolfair.ma)

**Financial Strength**



الشركة المركزية للاحتياط والتأمين  
*Société Centrale de Réassurance*  
GROUPE CDG

Tour Atlas - Place Zellaqa - B.O.Box 13183 - Casablanca  
Phone : +212 (05)22 46 04 00  
Fax : +212 (05)22 46 04 60  
E-mail : [scr@scrmaroc.com](mailto:scr@scrmaroc.com) - Web : [www.scrmaroc.com](http://www.scrmaroc.com)

# MOROCCO:

## Insurance Market Overview

by **Hussein Elsayed**  
Misr Insurance Company

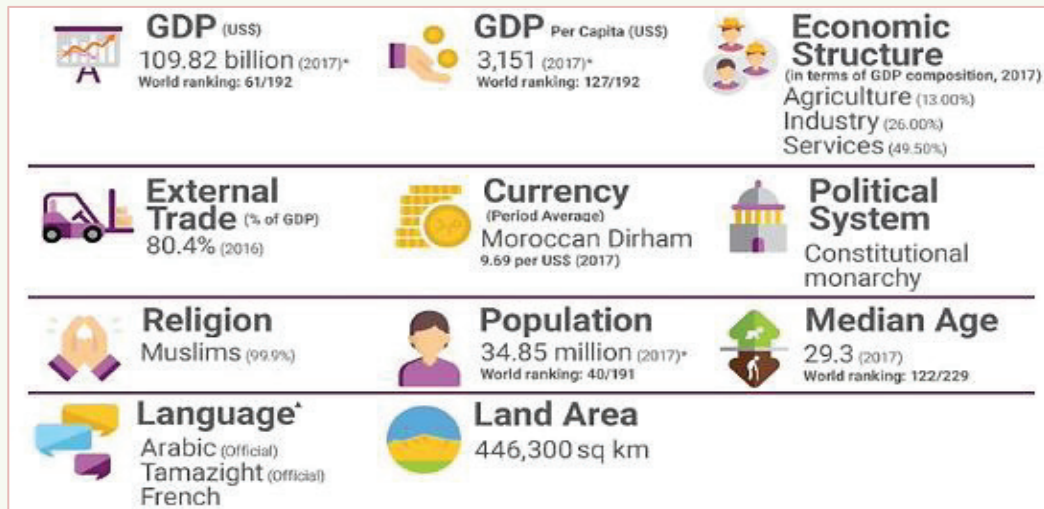


**Official Name:** The Kingdom of Morocco  
**Belongs to:** AMU, Arab League, IMF, UN

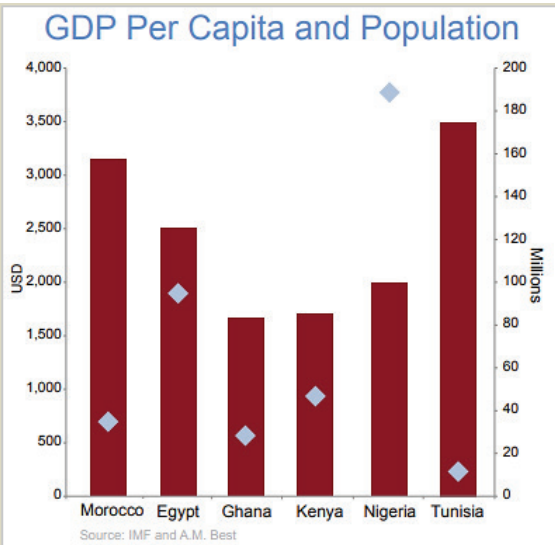
**Capital:** Rabat



### (I) MOROCCAN SOCIO-ECONOMIC DATA



	2013	2014	2015	2016	2017
Population (million)	33.4	33.8	34.1	34.5	34.9
GDP per capita (US\$)	3,143	3,346	2,976	3,012	3,119
GDP (US\$ bn)	105	113	102	104	109
Economic Growth (GDP, annual variation in %)	4.5	2.7	4.5	1.2	4.0
Consumption (annual variation in %)	3.2	3.1	2.3	3.4	4.2
Investment (annual variation in %)	-0.5	-1.3	0.2	9.3	-0.2
Industrial Production (annual variation in %)	0.9	1.3	1.6	2.1	2.6
Unemployment Rate	9.2	9.7	9.6	9.9	9.9
Fiscal Balance (% of GDP)	-5.1	-4.7	-4.2	-4.0	-3.6
Public Debt (% of GDP)	61.7	63.4	63.7	64.7	64.5
Money (annual variation in %)	2.7	5.0	7.0	6.3	7.8
Inflation Rate (CPI, annual variation in %, eop)	0.4	1.6	0.6	1.8	1.9
Inflation Rate (CPI, annual variation in %)	1.9	0.4	1.6	1.6	0.8
Policy Interest Rate (%)	3.00	2.50	2.50	2.25	2.25
Exchange Rate (vs US\$)	8.16	9.06	9.92	10.12	9.35
Exchange Rate (vs US\$, aop)	8.41	8.41	9.75	9.81	9.71
Current Account (% of GDP)	-7.9	-5.7	-2.1	-4.2	-3.6
Current Account Balance (US\$ bn)	-8.5	-6.6	-2.2	-4.4	-3.9
Trade Balance (US\$ billion)	-23.6	-21.2	-14.7	-17.8	-18.2
Exports (US\$ billion)	22.0	20.5	18.7	18.9	21.4
Imports (US\$ billion)	45.6	41.7	33.4	36.7	39.6
Exports (annual variation in %)	2.9	-7.0	-8.9	1.3	13.1
Imports (annual variation in %)	1.8	-8.7	-19.8	9.8	8.0
International Reserves (US\$)	18.8	20.2	22.7	25.0	26.1
External Debt (% of GDP)	37.9	38.8	43.1	45.5	48.1



**S&P Global Ratings**  
**Property/Casualty Insurance Industry And Country Risk Assessments**  
 On Sept. 25, 2018

**MOROCCO**

Country Risk	Industry Risk	IICRA
Moderate Risk	Low Risk	Moderate Risk

## Natural Hazards:

### Earthquake and Other Geological Hazards:

Morocco is located on an important fold belt of tectonic plates. Ground conditions include fertile coastal soft soil, volcanic rock and desert sand to the south.

The country is exposed to two zones of tectonic activity: one is in the region of the Rif and Atlas mountain chains; the other is the Azores-Gibraltar ridge, which is situated offshore in the Atlantic ocean.

The zones at risk are:

- coastal zone, including the cities of Tetouan, Tangier, Rabat, Sale, Casablanca and Safi
- interior zone, including the cities of Marrakech, Fes and Meknes.

Minor tremors of below 5 on the Richter scale occur with regularity.

### Windstorm

All coastal areas of Morocco are exposed to the weather fronts coming in from the Atlantic Ocean, but the country has been spared major storm losses, and windstorm is considered to be a smaller risk than earthquake or flooding.

### Flood

Floods are a major hazard in Morocco; indeed, they represented nine of the top ten natural disasters in Morocco between 2002 and 2012 in terms of average economic loss (The World Bank Group, 2018). The National Assessment of Disaster Management (Catastrophe Royaume du Maroc) carried out in 2016 identified floods as one of four priorities, along with, forest fires, earthquakes and locusts. Between 1995 and 2005 floods were responsible for more than 1,165 deaths, more than 232,896 affected population, and more than US\$ 295 million in damages.

### Hail

- Three hail corridors are recognised in Morocco:
- along the Middle Atlas mountain range
  - in the south-west of the country to the north of Marrakech
  - in the Meknes - Fes region.

Insurance is sought for export crops, such as apples and citrus in Middle Atlas areas, and bananas and tomatoes grown under glass around Agadir. Cover is available for the crops and for damage to greenhouses.

The agricultural mutual MAMDA writes a small amount of insurance against hail.





## (II) MOROCCAN INSURANCE MARKET



The Moroccan insurance market is the most sophisticated in Africa, after South Africa. Regulators now play a significant role in pushing down the base capital of companies, which has led to challenging conditions for some local firms. In a typical developed economy such as France, insurance is a €3000-per-capita business, while in Morocco it sits at €100-per-capita.

At some point it is reasonable to expect that Morocco will evolve into a genuine developed economy, and when that does occur the potential for business will be huge. At that point it is expected that all segments of the economy should grow positively, with health insurance leading the way.

The domestic market is evolving in a very positive trend, with growth of 10.9% in 2017, excluding reinsurance.

The life segment drove this trend, growing 18.8%, supported by the arrival of a new player – Taamine Chaabi – which helped to boost the product line over the last couple of years.

Meanwhile, the non-life segment experienced growth of 5.5% in 2017, and the net profit of insurers increased by 25%, a development the stock market reacted to well.

## Regulatory Framework

Much of the sector’s evolution over the coming years will be shaped by the implementation of Law No. 59-13, which introduces several significant regulatory changes to the market. The move was part of a broad revamp of Morocco’s insurance legal framework, which began in August 2016 with the long-awaited approval of a new Code des Assurances, or insurance law.

Although the sector was previously overseen by the Insurance and Social Welfare Directorate, a unit of the Ministry of Economy and Finance, the 2016 reforms led to the establishment of a new independent insurance sector watchdog, ACAPS. The new regulator has since been engaged in training and informing insurance brokers about the obligations of firms operating in the sector and customer protection requirements. Nevertheless, other elements of the reform package have taken somewhat longer to be fully implemented.

A notable element of this is the development of a regulatory framework for the issuance of takaful products. However, in February 2019 a draft bill for the regulation of the takaful segment was unanimously agreed upon by the House of Representatives, the lower house of the country’s Parliament, and was expected to be voted through by the upper house in early 2019.

Under the new framework, firms seeking to sell sharia-compliant services will have to offer takaful products exclusively, meaning only Islamic banks and new institutions established by conventional issuers will be able to operate in the segment. This move, which is expected to bring greater competition and diversification to the kingdom’s insurance market, will enable products including sharia-compliant life insurance, family insurance, mortgages, and insurance for property damage, accidents and automobiles.

As part of the reform of the sector, ACAPS is also working on new solvency rules for insurance companies. This new framework will be based on the EU’s Solvency II model, but with certain adaptations for the Moroccan market.



“Under the new regime, solvency margins will include all risks to which the company is exposed, rather than merely the subscription risk,” Amal Souafi, head of the research department at ACAPS, told OBG. As of early 2019 the regulator was still developing the framework and undertaking discussions with sector operators. “The ongoing change of the prudential rules will imply a change in the way insurance companies manage their funds. There should be a shift from placing money on shares to using more and more obligations, which represent a lower risk,” Abelilah Laamarti, managing director of SANAD assurances, told OBG.

### SUPERVISORY AUTHORITY:

**Insurance Control and Social Protection Authority**  
**Autorite de Contrôle des Assurances et de la Prévoyance Sociale**  
**ACAPS** [www.acaps.ma](http://www.acaps.ma)



### INSURANCE ASSOCIATIONS:

**Moroccan Federation of Insurance and Reinsurance Companies**  
**Federation Marocaine des Sociétés d'Assurances et de Reassurance**  
**FMSAR** [www.fmsar.org.ma](http://www.fmsar.org.ma)

**Committee of Marine Insurers of Morocco**

**National Federation of Agents and Insurance Brokers in Morocco**  
[www.fnacam.ma](http://www.fnacam.ma)

**Moroccan Association for Risk Management**  
[www.amrim.ma](http://www.amrim.ma)

### ➤ TYPES OF LICENCE

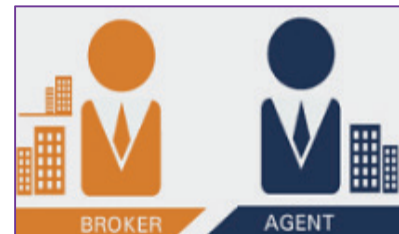
- Licences are issued by class, but until 2006 there was no requirement to have separate companies for short-term and long-term insurance. The Insurance Code, as modified by Law No 39-05, states that no further composite licences will be issued - although existing licensees were allowed to continue their operations on a composite basis.
- Personal accident and health are considered non-life classes but can also be written by way of riders by life insurers.
- Insurers can write inwards reinsurance without a separate licence.
- The launch of takaful is predicted to be likely to take place in 2019 and at that stage takaful operators entering the market will probably require distinct licences.

### ➤ FOREIGN OWNERSHIP

Foreign Ownership Under Law No 17-99 promulgated in 2002, foreign ownership of up to 100% of an insurance company licensed to do business in Morocco is permitted.

### ➤ BROKERS

- Under Law No 17- 99, brokers are required to be domiciled in Morocco, with at least 50% of their shares held by either Moroccan nationals or Moroccan-registered companies. They are also required to have professional liability insurance of at least MAD 1mn (USD 105,353).
- zMinisterial Order No 587-11, issued by the Ministry of Economy and Finance on 9 March 2011, contained updated requirements for insurance brokers' professional indemnity cover but did not specify new limits of cover.



### ➤ AGENCIES

- Agencies may work for only one insurance company. As a result of these restrictions some agencies have converted into brokers.
- Agents must be licensed by the regulator, and they must possess qualifications, which have become stringent. To obtain their licences, agents are required to pass a special exam or have 10 years' experience with a broker (or possess a university degree) and must spend at least six months training with the insurer on whose behalf they will issue policies.
- Under Law No 1 - 9, agents are required to have professional liability insurance of at least MAD 500,000 (USD 52,676).

### ➤ CAPITAL REQUIREMENTS

- Insurance and reinsurance companies must have a minimum capital of MAD 50mn (USD 5.27mn).
- This requirement applies equally to joint stock and to mutual companies but mutuals may be required to show a higher capital if the regulator considers this appropriate in view of the type of business the company intends to transact.



### ➤ SOLVENCY MARGINS

- Solvency margin provisions are contained in Law No 17-99 and follow EU Solvency I norms.
- For non-life business the minimum solvency margin is the higher of two calculations, one based on premiums and one on losses: both tests are based on the average of the last three years.
- The same solvency margin requirements apply to reinsurers. For the time being this solvency regime remains in force.

- Law No 59-13 of 25 August 2016 introduced general solvency (risk-based) principles, Risk based solvency will be progressively introduced up to 2021 accompanied by a structured implementation plan.
- Following the passing of Law No 59-13 a draft circular issued by the regulator in September 2018 is intended to introduce qualitative requirements in respect of the governance and risk management of insurance and reinsurance companies. The proposed regulations require regular audit of IT systems, self-assessment of risks which may impact solvency and emphasis on augmented actuarial functions as well as augmented oversight of other processes such as accounting and financial reporting, reserving, underwriting and claims management.



### ➤ RESERVE REQUIREMENTS

Under Law No 17-99 insurers are required to hold reserves equal to:

- Technical reserves sufficient to meet policyholder and client claims (no allowance is made for reinsurance ceded)
- Monies owed to preference creditors
- Reserves for repaying loans
- A fund corresponding to the technical reserves needed for the benefits scheme of personnel
- Deposits made by agents, clients and others.



### ➤ RETENTIONS

There are no rules limiting retentions.

### ➤ COMPULSORY INSURANCES

- Motor third party bodily injury and property damage (including complementary insurance for the transport of dangerous substances).
- Workers' compensation.
- Huntsmen's liability.
- Professional indemnity for certain categories of professionals, such as insurance agents, insurance brokers, accountants and architects.
- All property and motor insurance policies must cover damage caused by catastrophic events (natural catastrophes, SRCC and acts of terrorism).
- Construction all risks (CAR) insurance including third party liability of the principal, contractors, architects and engineers.
- Decennial liability insurance.
- Shipowners' liability for marine oil pollution (financial guarantee or insurance).



### ➤ STATUTORY TARIFFS:

- All compulsory tariffs have been discontinued.
- The tariff for motor third party liability was officially discontinued from 6 July 2006, but it is still used as reference. Segmentation of motor insurance risk rating must be based on technical requirements outlined by the regulator.

➤ **POOLS:**

There are currently no pools in Morocco.

➤ **NON-ADMITTED INSURANCE**

Non-admitted insurance is not permitted because the law provides that insurance must be purchased from local authorized insurers with some exceptions. Intermediaries (brokers or agents) are not permitted to place business with non-admitted insurers unless prior approval has been granted by the regulator.

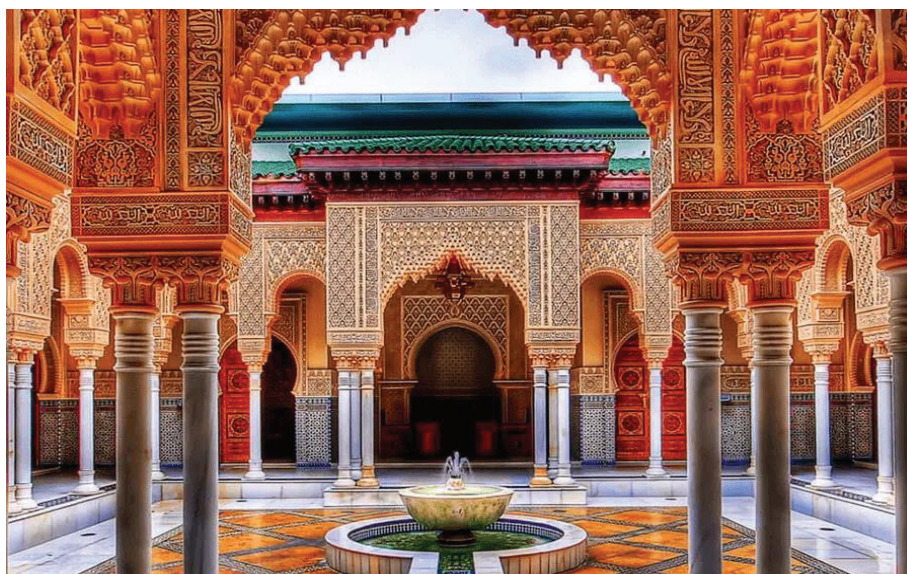


➤ **FRONTING**

- There are no regulations prohibiting fronting in Morocco. Following the implementation of Law No 17-99 insurers may make such arrangements, particularly if the risk concerned has unusually wide coverage or is excluded from reinsurance treaties.
- Fronting commission is set by negotiation but is typically around 5.0% or 7.5%. The insurance regulator will wish to see acceptable security on any fronting arrangement.

➤ **REINSURANCE BUSINESS:**

- There are two locally established reinsurers: **Societe Centrale de Reassurance (SCR)** which founded in 1960 and **MAMDA Re** which founded in 2015.
- (SCR), lost its right to a 10% compulsory cession on 1 January 2014, but has retained its state guarantee. The significance of this guarantee is that SCR is considered locally to represent first class security, and, of course it is also regulated by the same authority as local ceding companies.
- Africa Re is entitled to a 5% cession of all treaties, but this is not always transacted.
- Local insurers do write very small amounts of reinsurance.
- An overseas reinsurer does not have to be licensed or registered in Morocco. The regulator closely vets the security of reinsurers with which Moroccan insurers place reinsurance business.



## Insurance Market Performance and Statistics



### ➤ MARKET SIZE

In 2018, the insurance sector has twenty-three companies operating, including nineteen limited companies and four Mutual Insurance Companies:

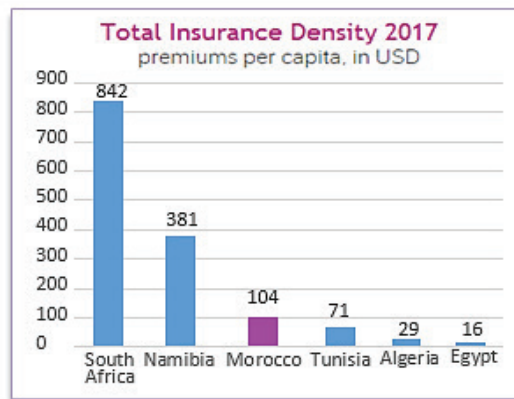
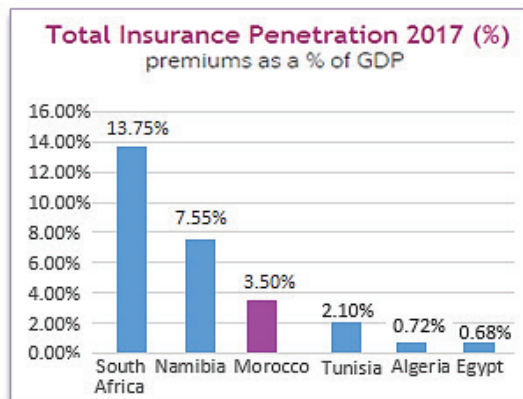
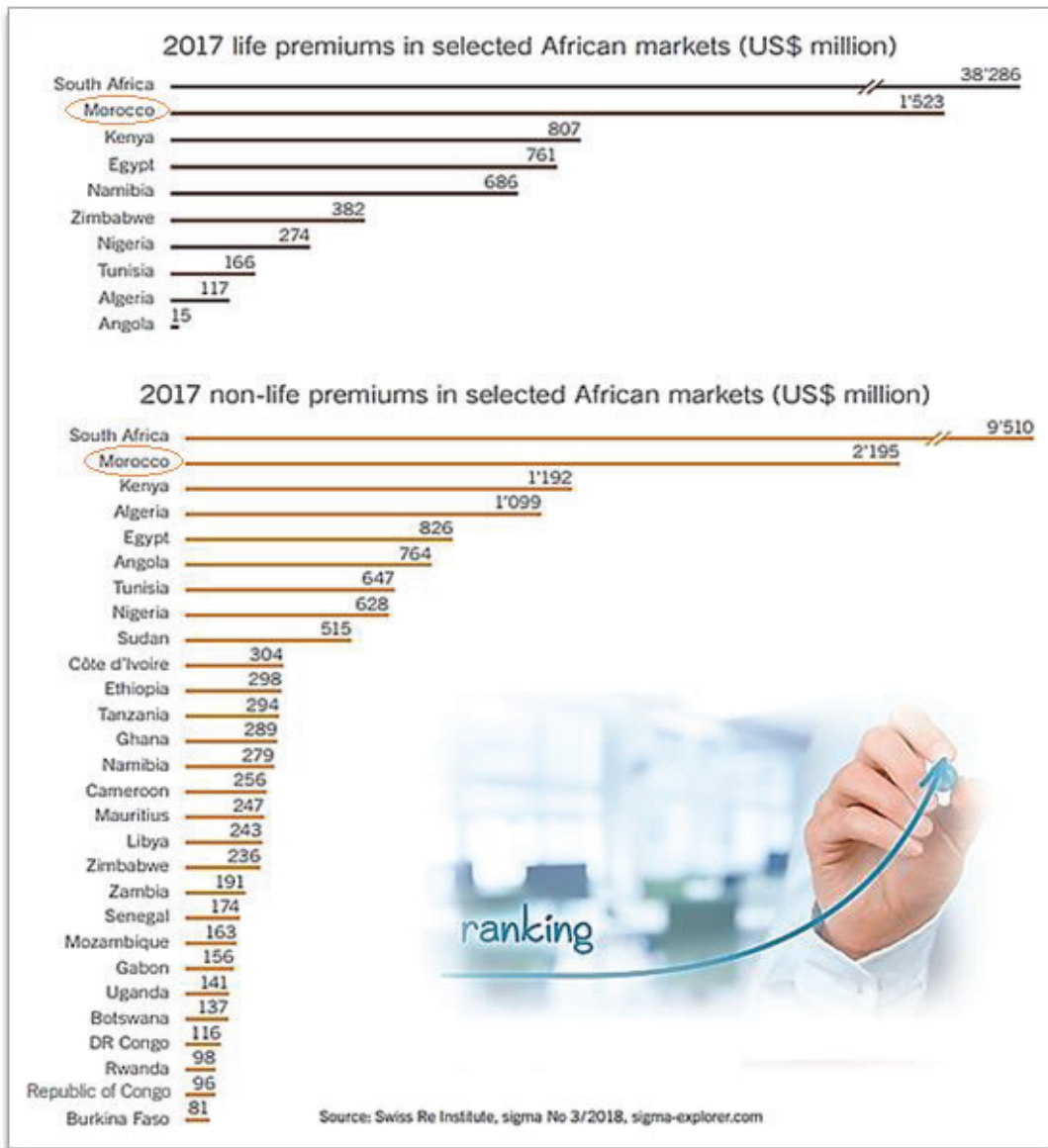
- 23 Insurance and Reinsurance Companies
  - 8 Companies practicing life, non-life and capitalization insurance operations
  - 3 Companies only practicing non-life insurance operations
  - 2 Companies only practicing life insurance operations
  - 5 Companies only practicing assistance operations
  - 3 Companies only practicing credit insurance operations
  - 2 Companies only practicing reinsurance operations.
- 1962 Agents and Brokers
- 580 direct offices
- 6209 Bank agencies (2017)

### ➤ GROSS PREMIUM 2013-2017

Total Premiums	2013	2014	2015	2016	2017
Total Direct Premiums (US\$ m)	3180	3381	3094	3561	3718
Real Premium Growth (%) inflation-adjusted	0.8%	5.9%	4.7%	13.7%	3%
Penetration (% of GDP)	3%	3.1%	3.1%	3.5%	3.5%
Density (per capita in US\$)	94	98	89	101	104
Share of Total World Premiums (%)	0.07%	0.07%	0.07%	0.08%	0.08%
Share of African Total Premiums (%)	4.52%	4.81%	4.88%	5.99%	5.57%
Life Premiums	2013	2014	2015	2016	2017
Life Direct Premiums (US\$ m)	1023	1118	1082	1457	1523
Share of Country Total Premiums (%)	32.17%	33.07%	34.97%	40.92%	40.96%
Real Premium Growth (%) inflation-adjusted	-4.5%	8.8%	10.6%	33.2%	3.1%
Life Penetration (% of GDP)	1%	1%	1.1%	1.4%	1.4%
Life Density (per capita in US\$)	30	33	31	41	43
Share of African Life Premiums (%)	2.14%	2.34%	2.53%	3.69%	3.39%
Non-Life Premiums *	2013	2014	2015	2016	2017
Non-Life Direct Premiums (US\$ m)	2158	2263	2013	2103	2195
Share of Country Total Premiums (%)	67.86%	66.93%	65.06%	59.06%	59.04%
Real Premium Growth (%) inflation-adjusted	3.6%	4.4%	1.7%	3.3%	3%
Non-Life Penetration (% of GDP)	2%	2.1%	2%	2.1%	2.1%
Non-Life Density (per capita in US\$)	64	66	58	60	61
Share of African Non-Life Premiums (%)	9.53%	10.00%	9.61%	10.55%	10.07%

\* Include PA&H Insurance


Source: Swissre Sigma Explorer



According to Market Size in 2017, Morocco is currently ranked at **50** in the world by total market size | **51** by life market size | **48** by non-life market size  
**2nd** Market in Africa in terms of premium volume  
**3rd** market in the Arab world in terms of premium volume


**THE MOROCCAN INSURANCE MARKET IN 2017:  
BREAKDOWN OF PREMIUMS PER CLASS OF BUSINESS**

Figures in millions MAD



	Premiums 2015	Premiums 2016	Premiums 2017	Evolution 2016/2017	2017 market shares
<b>Non life insurance</b>					
Motor	9514	9954	10482	5.3%	27%
Bodily injury and health	3360	3653	3922	7.4%	10.1%
Workmen's compensation	2091	2174	2223	2.2%	5.7%
Fire and natural elements	1312	1318	1332	1.0%	3.4%
Assistance - credit – guarantee	1181	1331	1415	6.3%	3.6%
Marine	552	578	605	4.7%	1.6%
Third party liability	544	550	549	-0.2%	1.4%
Engineering	394	329	242	-26.4%	0.6%
Non life acceptances	212	184	187	1.5%	0.5%
Other operations	701	735	979	33.3%	2.5%
<b>Total Non life insurance</b>	<b>19861</b>	<b>20806</b>	<b>21935</b>	<b>5.4%</b>	<b>56.4%</b>
<b>Life and capitalization</b>					
Savings	7485	11087	13634	23%	35%
Insurance in case of death	2581	2685	2735	1.9%	7%
Variable life assurance	460	494	585	18.5%	1.5%
Life acceptances	33	27	1	-98.3%	0%
Other operations	1	3	31	864.9%	0.1%
<b>Life and capitalization</b>	<b>10560</b>	<b>14296</b>	<b>16985</b>	<b>18.8%</b>	<b>43.6%</b>
<b>Grand total</b>	<b>30421</b>	<b>35102</b>	<b>38920</b>	<b>10.9%</b>	<b>100%</b>

Figures in millions US\$



	Premiums 2015	Premiums 2016	Premiums 2017	Evolution 2016/2017	2017 market shares
<b>Non life insurance</b>					
Motor	966	989	1124	13.7%	27.0%
Bodily injury and health	341	363	420	15.7%	10.1%
Workmen's compensation	212	216	238	10.2%	5.7%
Fire and natural elements	133	131	143	9.2%	3.4%
Assistance - credit – guarantee	120	132	152	15.2%	3.6%
Marine	56	57	65	14.0%	1.6%
Third party liability	55	55	59	7.3%	1.4%
Engineering	40	33	26	-21.2%	0.6%
Non life acceptances	21	18	20	11.1%	0.5%
Other operations	71	73	105	43.8%	2.5%
<b>Total Non life insurance</b>	<b>2015</b>	<b>2067</b>	<b>2352</b>	<b>13.8%</b>	<b>56.4%</b>
<b>Life and capitalization</b>					
Savings	760	1101	1461	32.7%	35.0%
Insurance in case of death	262	267	293	9.7%	7.0%
Variable life assurance	47	49	63	28.6%	1.5%
Life acceptances	3	3	0.1	-96.7%	0.0%
Other operations	0.1	0.3	3	900.0%	0.1%
<b>Total life and capitalization</b>	<b>1072</b>	<b>1420</b>	<b>1820</b>	<b>28.2%</b>	<b>43.6%</b>
<b>Grand total</b>	<b>3087</b>	<b>3487</b>	<b>4172</b>	<b>19.6%</b>	<b>100%</b>

Exchange rate MAD/USD as at 31/12: 2015=0.10158 2016= 0.09932 2017=0.10719

Source: Autorité de Contrôle des Assurances et de la Prévoyance Sociale (ACAPS)



➤ **2017 RANKING OF INSURERS IN MOROCCO ACCORDING TO TURNOVER**

Figures in millions

Ranking 2017	Companies	Class of business	2017 premiums		2016 premiums		2016/2017 evolution
			In USD	In MAD	In USD	In MAD	
1	Wafa Assurance	Composite	863	8050	726	7314	10.06%
2	Royale Marocaine d'Assurances	Composite	667	6224	582	5860	6.22%
3	Saham Assurance	Composite	519	4846	436	4392	10.34%
4	AXA Assurance Maroc	Composite	441	4111	390	3928	4.66%
5	Mutuelle Attamine Chaabi	Life	394	3678	272	2739	34.29%
6	Atlanta Assurances	Composite	243	2271	193	1939	17.13%
7	Sanad Assurances	Composite	206	1921	174	1751	9.70%
8	La Marocaine Vie	Life	185	1724	147	1484	16.15%
9	Mutuelle Centrale Marocaine d'Assurance	Composite	136	1269	131	1315	-3.48%
10	Allianz Maroc	Composite	134	1246	120	1212	2.80%
11	Mutuelle Agricole Marocaine d'Assurance	Non-Life	100	929	85	858	8.26%
12	Compagnie d'Assurance Transport (CAT)	Non-Life	72	670	63	634	5.69%
13	Saham Assistance	Non-Life	54	500	47	470	6.45%
14	Maroc Assistance Internationale	Non-Life	48	449	43.2	435	3.17%
15	Mutuelle d'Assurances des Transporteurs (MATU)	Non-Life	29.7	277	29	293	-5.46%
16	Wafa IMA Assistance	Non-Life	26.2	244	21	209	16.84%
17	Euler Hermes ACMAR	Non-Life	13	126	11	116	8.45%
18	AXA Assistance Maroc	Non-Life	12.8	120	10.6	107	11.78%
19	Coface Maroc	Non-Life	6	56	4.5	46	20.65%

Exchange rate as at 31/12/2016 - MAD/USD: 0.09932

Exchange rate as at 31/12/2017 MAD/USD: 0.10719



➤ **REINSURANCE COMPANIES**

	Turnover In thousands USD		Net Result In thousands USD		Shareholder's Equity In thousands USD		Combined Ratio %	
	2016	2017	2016	2017	2016	2017	2016	2017
<b>Société Centrale de Réassurance (SCR)</b>	235500	215580	25440	52730	223520	280730	94%	93%
<b>MAMDA Ré</b>	9493	12182	191	265	51318	62995	91.21%	93.18%



SCR's 89.3% of gross premium income was Moroccan business and 10.7% was foreign business.

AM Best's  
Credit Ratings

AMB#  
084052

ICR  
bbb

Outlook/  
Implication  
Stable

FSR  
B++

Outlook/  
Implication  
Stable



		2016	2017	2016	2017
Market Concentration					
	Top 5 Companies	85.62%	85.45%	68.82%	68.65%
	Top 10 Companies			91.55%	91.61%
Distribution Channels					
	Direct (%)	10%	10%	27%	26%
	Broker and Agents (%)	20%	18%	60%	60%
	Bancassurance (%)	70%	72%	11%	12%
	Other (%)	-	-	2%	2%
Total Assets for life & non-life		2016		2017	
	Total Assets (MAD mn)	188550.87		199573.07	
	Growth (%)	5.23%		5.85%	
Technical Reserves for life & non-life		2016		2017	
	Technical reserves (MAD mn)	54,749.46		54,634.31	
	% of direct written premium	265.46%		250.67%	
Investments		2015	2016	2016	2017
	Invested assets (MAD mn)	61,875.95	61,289.83	NA	NA
Expense Ratios		2016	2017	2015	2016
		9.69%	8.86%	30.47%	30.21%
Profitability		2016	2017	2016	2017
	Underwriting profit/loss (MAD mn)	(161.97)	(2,407.20)	776.81	553.25
	% of net earned premium	(1.15)	(14.34)	4.28%	3.21%
	Pre-tax profit/loss (MAD mn)	958.41	921.84	4,051.54	3,969.19
	% of net earned premium	6.80%	5.49%	22.34%	23.02%
Retention Ratio		2016	2017	2015	2016
		98.65%	98.82%	87.71%	87.19%

Source: AXCO Insurance Information Service

### BANCASSURANCE REPRESENTS 25% OF THE INSURANCE ACTIVITY IN MOROCCO

In 2017, bancassurance accounted for 25% of the insurance activity in Morocco. According to the Supervisory Authority for Insurance and Social Security (ACAPS), this contribution increased twofold between 2008 and 2017.

At least 70% of life and capitalisation (savings plans) business is sold through bancassurance, which has developed rapidly in recent years.

In total 11 banks are licensed to transact bancassurance operations. Overall in 2016 these banks generated some MAD 8.4bn (USD 884.97mn) in gross bancassurance (life and non-life) premium income, with a 23% market share of life and non-life premiums. Currently bancassurance is estimated to account for about 70% of all life and health insurance sales but bancassurance penetration in the non-life sector is lower.

Several banks have established their own captive insurance brokers to distribute life, health and non-life products.

## ► 2018 RESULTS OF THE MOROCCAN INSURANCE MARKET

According to the Moroccan Federation of Insurance and Reinsurance companies (FMSAR), the turnover of the Moroccan insurance market amounted to 41.345 million MAD (4.323 billion USD) in 2018, against 38.966 million MAD (4.149 billion USD) in 2017, an increase of 6.1%. This performance follows three years of a two-digit market evolution.



Non-life insurance reported 23.155 million MAD (2.421 billion USD) in written premiums with an annual growth of 5.3%.

This performance is higher than that of 2017 set at 4.7%. Non-life insurance accounted for 56% of the market. As for life and capitalization activity, it recorded 18.19 billion MAD (1.901 billion USD) in premiums, up by 7.1% compared to 2017. This growth rate is in sharp decline compared to the 35.4% achieved between 2016 and 2017.

The ranking of companies remains unchanged. Wafa Assurance still at the top with a turnover of 8.371 billion MAD (875 million USD) and a market share of 20%. The Royale Marocaine d'Assurance comes second with a turnover worth 6.543 billion MAD (684 million USD) and a market share of 15.8%. Saham Assurance ranks third with 5.223 billion MAD (546 million USD) in premiums and a market share of 12.6%.

It should be noted that these three companies alone account for almost half of the market premiums (48.4%).

## AFRICAN DRIVE

Following in the footsteps of Moroccan banks, three major Moroccan insurance companies have built up a presence in sub-Saharan African markets in recent years, particularly in francophone West Africa. Saham has by far the largest presence on the continent of any Moroccan insurer, with operations in 19 countries, as a result of its 2010 acquisition of pan-African insurance provider Colina and its purchase of a 100% stake in Mauritian non-life insurer Sun Insurance for an undisclosed amount.

Wafa and RMA, which in 2014 purchased a 40% stake in West African regional insurer Beneficial Life Insurance, each have a presence in four countries. November 2016 saw the official launch of Wafa Assurance's two Côte d'Ivoire units, a life and non-life firm, respectively, which received their licences from the local authorities the previous February.

The Moroccan insurance firms remained interested in expanding their presence in sub-Saharan markets; however, that recent regulatory changes by Central and West African insurance regulator Inter-African Conference on Insurance Markets (Conférence Interafricaine des Marchés d' Assurance, CIMA) could reduce the attractiveness of further expansion in the region. "CIMA recently tripled capital requirements, which will require firms to raise capital, and give rise to consolidation and other market changes, as well as requiring reinsurers to be physically present to operate in the region – both of which could impact profitability.





# قناة السويس للتأمين

---

## Suez Canal Insurance

# SCI

تأسست عام ١٩٧٩

**16569**  
Call Center

الثقة.. وراحة البال

المركز الرئيسي : ٣١ شارع محمد كامل مرسى - المهندسين - الجيزة  
تليفون : ٣٧٦٠١٠٥١ - ٣٧٦٠٦٨٦٨ فاكس : ٣٣٣٥٤٠٧٠ - ٣٣٣٥٠٩٨١



## 2018 FAIR Case Study Competition

### *Cyber Insurance And Risk Management: Closing The Gap*

**Prepared by: Kareem Mohamed Awad Elsayed - Cert CII**

Senior Property Underwriter

Arab Misr Insurance Group |gig

Email: awad.k@gig.com.eg

### Introduction

Modern communications and information technologies have become the backbone of each business and industry, the use of such technologies vary from different types (like cell phones, computers, Wi-Fi, electronic machines, etc.) that it have ceased to be the luxury item it was even 10 years ago and have become nowadays the basic absolute need and we cannot escape from, it has a very big role in most aspects of our lives. The importance of technology is aiming for comfort of use in whichever form it is.

It becomes more compact every year, offers more capabilities and top performance. The importance of technology in our daily basis is undeniable has inspired scientists to make improvements from time to time through their invented tools and devices for us to use, and no any organization can transit their business without reliance on technology regardless the size and type of business . It can perform multiple tasks simultaneously the operator can have many different programs running simultaneously even computers are generally able to perform complex calculations, such as math equations or travel distances, very quickly and accurately.

With use of technology in business transitions we have many tools available to us that make it easier to manage business's operations and exchange valuable information with the organization's customers and vendors. Since technology has developed so much from computer technology to mobile technology such innovations and new technologies are helped to bridge the gap to access in several markets around the world as there is no longer a void between people of one country and overcome those communication barriers before. It also has eliminated the bulkiness associated with paperwork; information can now be stored virtually in various storage devices such as compact disks and microchips. The technology helps companies to reduce costs by making a revision of business processes focus of projects focused on reducing costs to projects that develop innovative products and generate revenue. Both businesses and consumers have benefited from improvements driven by technology such as online ordering, traveling without obtaining tickets physically and inventory time management.

Due to the rapid growth of the technology the cyberspace has introduced numerous new threats and opportunities in their use and operations, stake holders of the organization are exposed to cyber security incidents of many different kinds and degrees of severity these include information theft, disruption of services, privacy and identity abuse, fraud, espionage and sabotage. At larger scale societies are threatened by possible attacks on critical infrastructure via cyber space as well as the potential for cyber terrorism and even cyber-warfare. The cyber space has brought societies to appoint where a very large number of the risks that we traditionally have been exposed to in the physical world today arise in cyberspace and have been cyber risk. In order to ensure a satisfactory level of cyber security, stake holders need to understand the nature of cyber risk what distinguishes cyber-risk for other kinds of risk and they need adequate methods and techniques for cyber risk management.

The objective of this study to address the several types of cyber risks and its risk management techniques including identify the plenty of the potential opportunities to insurers to shape cyber risk assessment, how the insurers handle and manage the portfolio of cyber-risks as well as the products and covers suitable for each industry or class of business.



## Chapter 1

### Cyber Risks and Threats

The digital world brings enormous benefits it is also vulnerable. Cyber security incidents be that international or accidental are increasing at an alarming pace and could disrupt the supply of essential services such as water supply; health care; electrical supply or mobile services. Cyber security involves the process that organizations need to put in place in order to address cyber risks. These are the risks to organizations (and ordinary people) caused by digital technology. These risks can cause damage to organizational assets including money; operational efficiency; organizational reputation, theft of money from online bank accounts, the theft of personal data for fraud purposes, deletion of data or compromise of computing machinery resulting in damage to business efficiency, damage to an organization's reputation caused by hijacking of social media accounts, the loss of strategic IP such as a new design due to the loss of a mobile device, or a failure to spot counterfeit goods being sold online. Therefore cyber security is accepted as a major issue around the world.

It is important to understand that cyber security needs to be managed across organization not only within the IT department but also to all the organization's employees to deal with cyber security. It is a major issue for organizations worldwide and there are many other major sources of danger from cyber technology such as wasted investments, the increased power of customers, reputational damage, the accidental sharing of strategic information, and the huge increase in compliance failures around data protection and other regulations.

Cyber risks can be caused by many things such as hacker, perhaps a criminal or a political activist, penetrating an IT network to steal data. As well as involve the accidental leakage of secret information or personal data caused by a careless or naive employee which may be caused to damage. This damage can be direct financial loss through theft or fines, reduced sales, operational disruption, increased recruitment, credit or supplier costs, a loss of competitive advantage or reputational damage.

In the 2017 Global Risk Management Survey by Aon Risk Solutions the Cyber Crime /Hacking/Viruses had ranked of the five positions among of the top 10 Risks in the terms of impact.

**Therefore the cyber security need for reliable method, tools and process for their risk management in general include risk assessment which will discussed in this chapter as follows:**

**Part 1: Cyber Risks and Cyber Security;** this part will introduce definition of the cyber risks, cyber security and their importance, different classification of the risks and their financially impact on business.

**Part 2: Cyber Systems and its Risk Management;** this part will introduce the cyber systems; cyber Resilience and the characteristics of them including the critical infrastructure protection and general process to cope security of cyber systems

## Part 1

### Cyber Risks and Cyber Security

In this part we will discuss the definition of the cyber risks, cyber security and their importance, different classification of the risks and their financially impact on business after an incident including their dimensions.

#### **1. The Definition Risk:**

Risk is considered the potential of an undesirable or unfavorable outcome resulting from a given action, activity, and / or inaction. The motivation for “taking a risk” is a favorable outcome. It can also define as (possibility of an unfortunate occurrence, doubt concerning the outcome of a situation, possibility of loss). Managing risk implies that other actions are being taken to either mitigate the impact of the undesirable or unfavorable outcome and / or enhance the likelihood of a positive outcome.<sup>1</sup>

Risk tolerance levels can be qualitative (for example low, elevated, or severe) or quantitative (for example, dollar loss, number or customers impacted, or hours of downtime). It is the responsibility of the Board of Directors and executive management to establish risk tolerance criteria, set standards for acceptable levels of risk, and disseminate this information to decision makers throughout the organization.<sup>2</sup>

#### **2. The definition of Cyber Risk:**

Cyber Risk is commonly defined as exposure to harm or loss resulting from breaches of or attacks on information systems related to technical infrastructure or the use of technology within an organization.

Events covered by this more comprehensive definition can be categorized in multiple ways. One is intent. Events may be the result of deliberately malicious acts, such as a hacker carrying out an attack with the aim of compromising sensitive information, but they may also be unintentional, such as user error that makes a system temporarily unavailable<sup>3</sup>. Risk events may come from sources outside the organization, such as cybercriminals or supply chain partners, or sources inside the organization such as employees or contractors.

Overs any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks.

It also encompasses physical damage that can be caused by cyber-attacks, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments.

---

<sup>1</sup> Chartered Insurance Institute ,*Insurance, legal and regulatory IF1 Study text: 2013-14,Ch1 Risk and insurance, Pages16-20*

<sup>2</sup> Becky Metivier,"How to Define Cyber security Risk", Website article ,Sage Data Security, Available from:<https://www.sagedatasecurity.com/blog/how-to-define-cybersecurity-risk>(Accessed 7th July 2018)

<sup>3</sup> Institute of Risk Management ,”Cyber risk”, Website article ,Available from <https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk.aspx>(Accessed 7th July 2018)



## 2.1. Information technology risk

While the information has long been appreciated as a valuable and important asset, the rise of the knowledge economy and the digital revolution has led to organizations becoming increasingly dependent on information, information processing and especially IT. Various events or incidents that compromise IT in some way can therefore cause adverse impacts on the organization's business processes or mission, ranging from inconsequential to catastrophic in scale.

## 3. History of Cyber Risk:

Over the past decade two major themes have boosted awareness around data protection, cyber risk/data loss incidents and widespread software vulnerabilities. With a long history stretching back as far as the HMRC CD-ROM debacle, which concerned 25m people, data loss incidents have continued to grow in prominence and frequency like the data loss from Adobe, Yahoo!, Sony, eBay and many more have had the public asking whether businesses are well enough equipped to secure their data. Simultaneously serious software vulnerabilities some of which are no doubt taken advantage of by hackers in many high-profile data breach incidents. Cyber-attacks are continuously evolving into smarter and unforgiving incidents they are forcing businesses into conjuring a three-part defense mechanism: prevent, detect and respond. Many high-profile cyber-attacks throughout the years have served as a reality check for corporate firms which essentially highlight that prevention and detection solutions are simply not enough<sup>4</sup>. Here the timeline of the recent cyber-attack:

### 3.1. The first worm – 1989:<sup>5</sup>

A computer worm is a malware computer program that replicates itself to spread to other computers, most of the time this type of malware uses a computer network to spread itself relying on security failures on the target computer to access it. In contrast to viruses which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help. 1989 saw the creation of the first computer worm to test the size of the internet. Unfortunately the manipulating virus spread aggressively essentially terminating the internet. The impact of the initial worm was not on the same level of devastation that could be created by harmful malware today. However, it was the first of many to come and shaped how viruses were managed for decades. Furthermore this motivates the businesses to invest in the first defensive security products, such as firewalls as it was first step for cyber security process.

### 3.2. The first viruses – 1990-99:

---

<sup>4</sup> Le VPN, "ORIGIN OF CYBER SECURITY: WHEN DID INTERNET PRIVACY BECOME AN ISSUE? "Website Article , Published on 2nd October 2017 , Available from <https://www.le-vpn.com/internet-privacy-cyber-security/> (Accessed 7th July 2018)

<sup>5</sup> Ted Julian, "Defining Moments in the History of Cyber-Security and the Rise of Incident Response", website article , Published on 4th December 2014, Available from <https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/> (Accessed 7th July 2018)

A computer virus is a type of malicious code or program written to alter the way a computer operates and that is designed to spread from one computer to another in contrast to worms viruses aren't standalone software and require a host program or human help to propagate. Melissa and ILOVEYOU were both fast-spreading macro viruses which were distributed as an e-mail attachment. When the attachment was opened, it disabled a number of safeguards in Word 97 or Word 2000. This malware infected numerous amounts of PCs and damaging email systems worldwide without a clear intention. This was the first issue of cyber-vandalism on a massive scale. These threats of viruses initially highlighted how employee mistakes can damage cyber security, therefore take action to remove the human element through technology. This was implemented using auto-updating anti-virus software designed to spot the signature of the virus and prevent it from executing.

### 3.3. Credit card cyber-attacks 2007:

Cyber-attacks become bigger with end-goals relating to financial benefits. Hacker Albert Gonzalez conducted an operation that stole information from nearly 50 million cards used by customers of US retailer TJX, costing the company USD 256 Million then businesses realized hackers could deceive their existing security tools and operate within their networks for years. This is one of the main reasons as to why detection solutions became a top priority for existing companies. Businesses learned the consequences of investing the minimum amount into their cyber-security and began arming themselves with more sophisticated security systems.

### 3.4. Target and Sony – 2014:

During 2014 there were massive recent data breaches of Target and Sony this situation emphasized that today's cyber-threat is ever-growing and reaching astonishing new heights. Cyber criminals took their skills to new levels whether they were individuals or part of a criminal organization. This time round there was a lot more at risk than money; company reputation and jobs were lost in the process. Target booked \$162 million in expenses throughout 2013 and 2014 related to the **data** breach, in which hackers broke into the company's network to access credit card information and other customer data, affecting some 70 million customers.

### 3.5. Biggest Ransomware Outbreak 2017:

The attack saw the likes of the NHS and FedEx dismantled. Spanish telecommunications company Telefonica was among many targets in the country along with German railway operator Deutsche Bahn<sup>6</sup>.

---

<sup>6</sup> NATO Review, "The history of cyber-attacks", website article, Available From <https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm/>(Accessed 7th July 2018).

#### 4. Cyber Security :

Cyber security involves the steps organizations need to take in order to address the risks they face from their use and their employees' use of digital technology especially IT networks, the Internet and mobile devices. Cyber refers to computers as defined digital security in that modern computers are driven by digital technology. Cyber security is a major issue for organizations worldwide according to the Center for Strategic and International Studies total global losses from cybercrime are probably at least USD 400 billion annually and cybercrime losses at UK retailers totaled £505 million in 2013. There are many other major sources of danger from cyber technology such as wasted investments, the increased power of customers, reputational damage, the accidental sharing of strategic information, and the huge increase in compliance failures around data protection and other regulations.<sup>7</sup>

Cyber risks can be caused by many things, they can involve a hacker perhaps a criminal or a political activist, penetrating an IT network to steal data but they will just as often involve the accidental leakage of secret information or personal data caused by a careless or naive employee, the theft of information caused by a disaffected employee who is planning to join another organization, or reputational damage caused by unhappy members of the public using social media and the result can be major damage. This damage can be direct financial loss through theft or fines, reduced sales, operational disruption, increased recruitment, credit or supplier costs, a loss of competitive advantage or reputational damage. It is important to understand that cyber security is not just about managing the risk to computer networks from hackers or from equipment failure these are important risks, generally managed by the IT department or an outsourced supplier but risks that cyber security processes need to manage extend far beyond this and can be found across organizations.

Generally many of these sorts of incidents will be outside the IT department's area of responsibility, which is why they need to be understood by the board and management generally. This isn't to say that IT security shouldn't be at the center of any cyber risk management process. Of course it should. But the risk management process needs to go way beyond IT system security.

#### 5. The Importance of Cyber Security:

Cyber security is constantly growing in importance as almost of the organizations are operating online and so becoming more reliant on the Internet, therefore the effective cyber security is necessarily to protect a network and website or a server. The organizations should have at least the minimum cyber security requirements like (Endpoint Protection, Firewall, Intrusion Detection System / Intrusion Prevention System, Web Filtering Software, Radius Server, Logging Software, Encryption)<sup>8</sup>. Businesses can incur huge fines for failing to protect and handle data effectively in order to keep their data secure.

---

<sup>7</sup> Green, Jeremy Swinfen, "Cyber Security: An Introduction for Non-Technical Managers", Routledge. 2015, eBook.; Pages 8-12

<sup>8</sup> The European Centre of Technology, "THE IMPORTANCE OF CYBER SECURITY", Website article, Available from <https://theect.org/importance-cyber-security/> (Accessed 8th July 2018).

## 6. Different classifications of the cyber-attacks and risks :

### 6.1. Types of Cyber -attacks<sup>9</sup>:

#### 6.1.1.1. Socially engineered malware:

Is often led by data-encrypting ransomware otherwise innocent website is temporarily compromised to deliver malware instead of the normal website coding. The maligned website tells the user to install some new piece of software in order to access the website then run fake antivirus software or run some other critical piece of software that is unnecessary and malicious, the user is often instructed to click past any security warnings emanating from their browser or operating system and to disable any pesky defenses that might get in the way.

#### 6.1.1.2. Password phishing attacks:

Approximately 60 to 70 percent of email is spam, and much of that are phishing attacks looking to trick users out of their logon credentials. Fortunately anti-spam vendors and services have made great strides so most of us have reasonably clean inboxes. The primary countermeasure to password phishing attacks is to have logons that can't be given away. This means two-factor authentication (2FA) smartcards biometrics and other out-of-the-band (e.g., phone call or SMS message) authentication methods.

#### 6.1.1.3. Unpatched software:

A browser add-in programs like Adobe Reader and other programs people often use to make surfing the web easier. It's been this way for many years now but strangely

#### 6.1.1.4. Social media threats:

The social world led by Facebook, Twitter, LinkedIn or their country-popular counterparts are threats usually arrive as a rogue friend or application install request. Corporate hackers love exploiting corporate social media accounts for the embarrassment factor to glean passwords that might be shared between the social media site and the corporate network. Nowadays worst hacks started out as simple social media hacking.

#### 6.1.1.5. Advanced persistent threats:

Only one corporation that has not suffered a major compromise due to an advanced persistent threat (APT) stealing intellectual property, APTs usually gain a foothold using socially engineered Trojans or phishing attacks. A very popular method is for APT attackers to send a specific phishing campaign-known as spear phishing- to multiple employee email addresses.

---

<sup>9</sup> Roger A. Grimes., "The 5 types of cyber-attack you're most likely to face", website article, Published on 21st August 2017, Available from <https://www.csoonline.com/article/2616316/data-protection/the-5-types-of-cyber-attack-youre-most-likely-to-face.html/> (Accessed 8th July 2018).

## 6.2. Types of CYBER-RISKS<sup>10</sup>:

There are different types of cyber risks, it relate to different classifications which can categories to system risks, people and network and cloud computing, the below notes considered list of the main risks:

### 6.2.1.1. Denial of service:

When an attack prevent the user temporarily from using resource, classic Internet DOS attacks temporarily block access to targeted servers by flooding them with traffic.

### 6.2.1.2. Pillage:

This is the risk of physical attacks or damage traditionally the term refers to physical destruction and is rarely used to refer to cyber- attacks. Equipment theft is probably the most common type of physical attack, and it clearly affects availability.

### 6.2.1.3. Subversion:

These risks affect the integrity of computer data and software through non-physical access.

### 6.2.1.4. Masquerade:

This risk reflects an authentication failure the attacker takes on a legitimate and/or privileged role within the computing system.

### 6.2.1.5. Forgery:

This applies a masquerade to individual messages; the attacker creates or modifies a message that the recipient misinterprets as being legitimate. Authentication is a complex process and is often omitted in lower-level network protocols and all network protocols try to make forgery difficult or impossible, but the techniques can fail.

### 6.2.1.6. Disclosure:

This risk is a classic failure of confidentiality. While disclosure may arise from a passive (eavesdropping) attack, it may also arise from other risks.

### 6.2.1.7. People:

Managing people requires a combination of documented guidelines and policies (so that people know what they should do), training, monitoring, and disciplinary processes (so that people understand the sanctions that will apply if they fail to follow guidelines and policies)

---

<sup>10</sup> Green, Jeremy Swinfen, "Cyber Security: An Introduction for Non-Technical Managers", Routledge. 2015, eBook.; Pages 38-42

## 7. The Dimensions of cyber-Risks including introduce of their impact on business after an incident<sup>11</sup>:

In case of happened of such cyber-attacks, these will be result of chain of events and losses sustained by organization, it will relate to such as (Security, Costs, Reputation, Liability, Compliance & privacy) which can be considered the dimensions of cyber risk and the possible costs after an incident can be classified as follows:

### 7.1. Impact on Business:

Such as Data and system recovery, System updates to prevent future incidents, Production interruption, Forensic investigations, Incident response and Redesign of critical infrastructure.

### 7.2. Liability:

Such as Losses payable to third party, revenue losses, Notifications, call center, costs, postage, Credit monitoring, Identity restoration, Infringement of trademarks.

### 7.3. Legal implications:

Such as Law suits (from vendors, customers, business partners) ,Legal advice, defense costs, fines.

### 7.4. Miscellaneous:

Such as Loss of revenue, Loss of contracts, Reputational damage, Share price impact, reduced sales, Future sales impact, Extortion payments, Public relations costs, Devaluation of intellectual property.



<sup>11</sup> Heidi A. Strauß, "Cyber Risks(Threats – Trends – Mitigation)", Training presentation, 2018 Münchener Rückversicherungs-Gesellschaft, Munich 12nd June 2018 Pages 5-8

## Part 2

### Cyber Systems and its Risk Management

In this part will discuss the cyber systems, cyber Resilience and characteristics of them including the critical infrastructure protection and general process to cope with the cyber system secure.

#### **1. Cyber Systems:**

Cyber Systems are a system that makes use of a collection of interconnected computerized networks including services, computer systems, embedded processors and controllers as well as information in storage or transit which may include information infrastructure, people and other entities that are involved in the business processes and other behavior of the system. This means that cyber-systems are part of the organizational structure of most organizations and consider the mechanism controlled or monitored by computer-based algorithms

In cyber-physical systems, physical and software components are operating on different spatial and temporal scales, exhibiting multiple and distinct behavioral modalities, and interacting with each other in a myriad of ways that change with context.<sup>12</sup>

##### **1.1. Cyber Resilience:**

Cyber resilience refers to an entity's ability to continuously deliver the intended outcome despite adverse cyber events. The concept essentially brings the areas of information security, business continuity and (organizational) resilience together. Organizations with potential need of cyber resilience abilities include but are not limited to IT systems, critical infrastructure, business processes, organizations and societies. The objective of cyber resilience is to maintain the entity's ability to deliver the intended outcome continuously at all times.

In order to build a cyber-resilient organization capable of withstanding or recovering from cyber-attacks, there are five inter-connected domains need to be used to guide a concerted program (Identify in order to develop an organization's understanding and management , Protect to covers all activities that will develop/update and implement effective precautions , Detect to identify any cyber security events, Respond to a detected cyber security event; Recover to how to plan a strategy to recover)<sup>13</sup>

##### **1.2. The characteristics of Cyber Security System :**

The successful information security policy establishes what must be done, why it must be done, how an organization is going to protect its information assets and information systems, ensure compliance with

<sup>12</sup> Refsdal Atle-Solhaug Bjornar-Stølen Ketil, "Cyber-Risk Management", EBook, Springer 2015, Pages 25-26

<sup>13</sup> Continuity central, "How to develop a Cyber Resilience Framework", Website Article, Published on 26th May 2017, Available From <https://www.continuitycentral.com/index.php/news/technology/2023-how-to-develop-a-cyber-resilience-framework> (Accessed 9th July 2018).

legal and regulatory requirements, and maintain an environment that supports the guiding principles<sup>14</sup> to be successfully implemented and include all relevant parties taken into consideration organization objectives and environmental impacts and global cyber threats.

## 2. Cyber Risk Management Definition :

Risk management is the ongoing process of identifying, assessing, and responding to risk. In order to manage risk organizations should assess the likelihood the potential impact of an event and then determine the best approach to deal with the risks: avoid, transfer, accept, or mitigate. To mitigate risks an organization must ultimately determine what kinds of security controls (prevent, deter, detect, correct,) to follow and apply. Not all risks can be eliminated and no organization has an unlimited budget or enough personnel to combat all risks. Risk management is about managing the effects of uncertainty on organizational objectives in a way that makes the most effective and efficient use of limited resources.<sup>15</sup>

It should be based on the organization's risk management frame work and its process must be decided as a part of the overall organization management. This frame should include policy, responsibilities and the integration of several parties into the organization and mechanism for internal and external communication; it should also continuously monitor and reviewed. The role of the risk management at the organization to help to reduce the impact of the incidents to the business's system operator by identify the appropriate treatment of risk as well as to comply with the laws and regulations concerning the risk management which allows risk decisions to be well informed and made in the context of organizational objectives.

## 3. Cyber Risk Management Considerations and Features<sup>16</sup>:

There are several considerations which have to be taken into account by the risk manager for Cyber Risk Management including when planning a risk management program such as aligning organization risk management to goals and objectives and sets the foundations for the program by establishing the three pillars of cyber risk management: governance, risk appetite, and policies and procedures.

In addition the risk manager has to consider the following when planning cyber risk management processes through (establish a culture of cyber security and risk management throughout the organization, communication processes and Information sharing, prioritize the risks, manage the speed response , risk identification)in order to maintain the a repository of up-to-date information for the cyber threats and vulnerabilities. Therefore the previous considerations it is essential to establish all in order to eliminate such risks.

---

<sup>14</sup> Becky Metivier, "Seven Characteristics of a Successful Information Security Policy", website article, Published on 8th February 2016, Available from <https://www.sagedatasecurity.com/blog/seven-characteristics-of-a-successful-information-security-policy/> (Accessed 9th July 2018).

<sup>15</sup> Refsdal Atle-Solhaug Bjornar-Stølen Ketil, "Cyber-Risk Management", EBook, Springer 2015, Pages 33-35

<sup>16</sup> Hillson, David, "The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk"; London: Kogan Page. 2016 EBook, Pages 34-40



#### 4. Cyber Risk Management Program Steps :

Making an efficient cyber risk management program in organization requires specific structures regardless of its framework, as a program consists of identification, evaluation, treatment and monitoring of risks. An important factor here is the interdisciplinary in the risk management team it is the only way to understand the criticality of the data being processed there are specific procedures and techniques provided the guidance and direction for the cyber risk assessment and each step has specified purpose as mentioned in the following steps:

##### 4.1. Align the Risk Management process to organization's goals and objectives<sup>17</sup>:

Ensure the risk manager role to work on maximize the potential goals of organization through examine strategic objectives by regularly considering how uncertainties for both risks and opportunities that could affect the organization's ability to achieve its goals which is critical process to maximize the stakeholders value.

##### 4.2. Risk Identification :

Assemble a comprehensive list of risks, both threats and opportunities that could affect the organization from achieving its goals and objectives. The identification of the risk sources which relate to strategic objectives is important to specify that risks either can be opportunities or threats accomplishing strategic objectives. Risks to objectives can often be grouped by type or category which focusing on the malicious and non-malicious cyber risks based on the nature of threat, threat source and vulnerabilities, how to approach their identification through analysis the initiate attacks, what motivates them, what their capabilities and intentions are and how attacks can be launched or investigate how the information is stored and processes in the system which applications and users have access to read or modify the information in case of non-malicious classification<sup>18</sup>.

##### 4.3. Risk analysis:

Examine risks considering both the likelihood of the risk and the impact of the risk on the mission to help prioritize risk response by assigning the likelihood of the risk's occurrence and its potential impact for the business result. It is important to use the best information available and techniques for threat modeling to describe aspects of attack prerequisites and make the risk assessment as realistic as possible and the risks are ranked based on organizational priorities in relation to strategic objectives<sup>19</sup>. Organizations need to be familiar with the strengths of their internal control when assessing risks to determine whether the likelihood of a risk event is higher or lower based on the level of uncertainty within the existing control methodology, these estimates serve as a basis for achieving the main goal of risk assessment to estimate the risk levels, cause of threat and vulnerabilities.

<sup>17</sup> MELISSA STEVENS, "4 Crucial Cyber Risk Management Steps Your Company Should Take Right Now", website article, Published on 31st May 2016, Available from <https://www.bitsighttech.com/blog/proactive-cyber-risk-management> (Accessed 19th July 2018).

<sup>18</sup> Refsdal Atle-Solhaug Bjornar-Stølen Ketil, "Cyber-Risk Management", eBook, Springer 2015, Page 34-42

<sup>19</sup> Green, Philip E. J.; Enterprise Risk Management: A Common Framework for the Entire Organization; Oxford: Butterworth-Heinemann. 2016; eBook, Pages 91-109

#### **4.4. Evaluation of cyber risk:**

This step can be done through four tasks as (Consolidation of risk analysis results which focus on the cyber risks based on uncertainty that may affect the risk level or decision making taken into account both the malicious and non-malicious threats together, Evaluation of the risk level , Risk aggregation and Risk grouping)

#### **4.5. Risk Treatment :**

The process of the risk treatment involve the features relate of the highly technical nature of cyber systems ,the sociotechnical aspects and human involvement .The risk treatment response based on risk appetite including acceptance, avoidance, reduction, sharing, or transfer. The risk manager review the prioritized list of risks and select the most appropriate treatment strategy to manage the risk when selecting the risk response<sup>20</sup>, it is important to involve stakeholders that may also be affected, not only by the risk but also by the risk treatment taken into consideration costs and benefits. The risk response should also fit into the management structure, culture and processes.

#### **4.6. Monitoring and review of Cyber Risk Management:**

As the cyber risks and attacks are continuously evolving and fast-changing environment the process of risk management here is required to be more dynamic than any conventional risk management process it must be largely computerized, therefore monitor how risks are changing and if responses are successful to help ensure that the entire risk management process remains current and relevant. This not only include how risk management are planned and conducted but also how and what extent measures and controls are implemented and how information is obtained and communicated.

#### **4.7. Communicate and Report on Risks:**

Communicating and reporting risk information to inform organizations stakeholders regarding the status of identified risks and their associated treatments, communicating risk information through a dedicated risk management report or integrating risk information into existing organizational performance management reports, such as the annual performance may be useful ways of sharing progress on the management of risk. The risk manager should have in place plans and procedures for how to provide, share ,obtain and make use of the information which need increased focus for there potentially adverse effect.

### **5. Cyber Risk Management Framework :**

#### **(How the Company managed to protect itself against different types of cyber risks and attacks)**

The Risk Manager of the organization need to understand importance to ensure that appropriate strategies are in place to provide a structure for managing and mitigating cyber risk. Importantly these strategies need to accept that cyber risk isn't simply confined to computing equipment owned by the

---

<sup>20</sup> Hampton, John J.; "Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity"; Ed.: Second edition. New York: AMACOM. 2015; eBook, page 234

organization as well as managing cyber security is not only imply a tactic of the IT department .It extend to all organization members in order to achieve this rule there are basic principles to be effective within the whole organization as follows :

### **5.1. Set of Cyber Security Strategy:**

The set of effective cyber security strategies need to be (holistic which involving all elements of an organization not just the computer network, appropriate where the most effort needs to be spent to defend against risks and where risks are acceptable, effectively sponsored by senior people who have a view of the whole business and not just one function, agile which constantly being revisited and updated in the face of a rapidly changing technological environment and finally engaging communicated to the whole organization)<sup>21</sup>.

The involvement of organizational leadership is essential if cyber risk is to be managed effectively. It is not just that risk management is part of corporate governance, It is because the attitude of leaders will affect how seriously people throughout an organization take cyber security as well as most organizations will need to rely on specialists to ensure that technical cyber risks are being managed for instance through constantly updated virus checkers and fraud site databases.

### **5.2. Picking the Right Team:**

The cyber threats occur across organizations not just in the IT department a good team will need an effective leader from across the organization whose have knowledge with a good understanding of the business able to understand the very different nature of different cyber risks occurring as a result of technology failures, pragmatic and able to choose actions that are underpinned by common sense and that are achievable by the organization.

The cyber risk leader<sup>22</sup> have to accountability for managing risk, it is likely that most cyber incidents have a number of different causes as these causes can be categorized as technology, business process and people causes. This may appear to be a technological risk best solved by software but there can be a people element to it as may be someone has uploaded malware to an office computer after a phishing attack and there could be a process element to it for instance the use of a weak password or a failure to control access to the network.

### **5.3. Getting prepared for the Risk Management Process:**

Getting prepared won't stop a cyber-security incident it just only will reduce its impact, therefore a comprehensive and well-documented process needed to ensure that everyone know what they should be doing at all stages of a crisis. The qualified leader at the organization should be able to predict many risk scenarios involving ranking potentially damaging incidents and its impact while some incidents (such as attempted network intrusion) may require considerable technical sophistication others may be

---

<sup>21</sup> Ulsch, N. MacDonnell; "Cyber Threat! : How to Manage the Growing Risk of Cyber Attacks"; Wiley Corporate F & A Series; Hoboken, New Jersey : Wiley. 2014; EBook, Page 127-145

<sup>22</sup> Zainudin, Dyana1;Ur-Rahman, Atta1;"THE IMPACT OF THE LEADERSHIP ROLE ON HUMAN FAILURES IN THE FACE OF CYBER THREATS.", *Journal of Information System Security*. 2015, Vol. 11 Issue 2, p89-109. 21p.

detected through social media buzz monitoring or reports from third parties such as consumers saying website isn't responding<sup>23</sup>. A key part of the prediction process is having the ability to decide if a damaging cyber incident is happening and, if so, what sort of response is needed.

The response plan once an incident has been detected will be activated to mitigate the threats, the intention should be to enable organization to have preparations in place that will prevent damage, limit damage, or enable a quicker recovery.

**5.4. Set of cyber risks register and its development:**

Identifying the types of cyber risks and how potential problems can occur is vital while the organization is going to create plans for managing cyber risks, there are a number of techniques that we can use to identify possible problems through "what if" scenarios which identify some unwanted events such as network penetration and work back to see how these events might occur, identify critical information and ways it might be compromised or leaked as well as document all cyber breaches that have happened in the organization before.

Due to the rapidly moving nature of digital technology managing risks considered difficult but strategies for doing this are emerging which include crisis assumption that assuming that critical incidents will happen regularly and therefore acting to protect critical infrastructure and build in buffers and Brains trust that creating a team of people from across the organization whose role is to identify potential existential crises. Therefore once the threats had been identified, evaluate each threat against the vulnerability of the system as it is at the moment to then it shall be identified what is the likelihood of damage occurring and what would the cost of this damage be as well as identify and select additional security controls to eliminate the risks or lower them to an acceptable level.

Then the quantifying Cyber risks is the next step based on the probability of the events impact of the organization, there is no one correct way of quantifying cyber risks but we could consider a 3- or 5-level scale in order to determine the risk rating based on the following equation: Impact (if exploited) \* Likelihood (of exploit in the assessed control environment) = Risk Rating

Using the values for impact and likelihood in the NIST Special Publication 800-30, here's what a completed risk rating Assessment:

Identified Threat	Impact	Likelihood	Value	Risk Calculation
Unauthorized Access (Malicious or Accidental)	High [100]	High [1.0]	100*1.0=100	Severe
Misuse of Information by Authorized Users	High [100]	Medium [.5]	100*.5=50	Elevated
Data Leakage / Unintentional Exposure of	High	Medium	100*.5=50	Elevated

<sup>23</sup> Green, Jeremy Swinfen, "Cyber Security: An Introduction for Non-Technical Managers", Routledge. 2015, eBook.; Pages 175-180

Customer Information	[100]	[.5]		
Failed Processes	High [100]	Low [.1]	100*.1=10	Low (Normal)
Loss of Data	High [100]	Low [.1]	100*.1=10	Low (Normal)
Disruption of Service or Productivity	High [100]	Low [.1]	100*.1=10	Low (Normal)

[Source: NIST Special Publication 800-30 /through Becky Metivier;"6 Steps to a Cyber security Risk Assessment", website article, Published on 11st April 2017, Available from <https://www.sagedatasecurity.com/blog/6-steps-to-a-cybersecurity-risk-assessment> (Accessed 21st July 2018).]

There are also questions help with estimating probability like how often have these or similar incidents happened in the past and to what extent have we fixed the cause of these incidents, have got any data that might throw light on these risks (e.g. the number of attempted penetrations each month) and is this data reliable and enough to analysis statistically. In this situation the decision in the risk register has been made that the risk is sufficiently important to require further mitigation.

#### 5.5. Management the impact of cyber security breach including the organization response:

The rule of risk manager to nominate to the senior managers one of the best solutions in respect of the risk treatment while managing cyber risks to include the following options:

Avoid risk through remove the risk through the elimination of the activity or situation that presents the risk as per the several ways<sup>24</sup>(Back up on a monthly basis and test the backups to ensure that the is well , Ensure files are properly destroyed and not simply deleted and dispose of devices only after they have been wiped clean of data ,strengthen passwords , Restrict access by allowing employees access only to information that is necessary for their tasks, restrict what they can do with information; ensure employees have to log on to access information, Update software such as firewalls, browsers and VPNs are regularly updated , delete unused software or store it outside the system and Educate employees to use common sense and follow guidelines about cyber security and social media especially about the risks of phishing and malware).

The remaining options are Transfer risk through Load the risk onto a third party through insurance, leasing equipment, or contract wording which will deeply discussed in the next chapter or to Reduce risk through minimize the likelihood or impact of the incident through processes and resources, etc. or finally Retain risk through accept that some risks are inevitable or not cost-effective to manage.<sup>25</sup>

All of the above risk treatment options differ from the costs, benefits, the security level at organizations and the precautions that had been taken through the organization to prevent or reduce the impact of such cyber threat to the performance of organization

<sup>24</sup> <sup>24</sup> Green, Jeremy Swinfen,"Cyber Security: An Introduction for Non-Technical Managers",Routledge. 2015,eBook.;Pages 191-199

<sup>25</sup> Chartered Insurance Institute, Reinsurance P97 Study text: 2015-16, Ch1 Purpose of and the parties involved in reinsurance, Page 5

In case of the cyber threat had happened to the cyber security system the process of responding to deal with this incident has two stages containment which is designed to contain any danger in order to give the organization time to react in order to limit damage and then elimination of the threat.

The rule of all organization members to contain any damage and recover any data lost or repairs any systems that have been damaged, they also need to be aware of the potential for other incidents as the initial incident may be a distraction designed to weaken the organization

The risk management team can make it easier to decide what actions are appropriate by asking the following questions: what happened? When and where did it happen? To whom did it happen? How did it happen? What were the main causes? What is the result of the incident? How much damage has been caused? and so on.

Once these questions have been answered the risk management team can discuss and decide on the next actions that need to be taken based on the risk treatment option have been taken by the senior leaders of the organization.



## Chapter 2

### Cyber Insurance Market

In the previous chapter we introduced the available options of risk treatment of cyber risks and threats from the organizations side, one of this options which is reliable and best treat with the cyber risk is risk sharing or transfer by sub-contracting or insurance which transfer of financial risks associated with the network and computer incidents to a third party. Cyber insurance is particularly effective option when the cost of additional information security controls does not reduce the risk enough to make the investment in such controls practical. Cyber insurance itself is not a defense without a rudimentary information security management system implementing all the requisite precautions, there is a growing market for cyber risk insurance for instance to reduce the uncertainty as this type of protection refers to monetary loss caused by network attacks and the financial compensation from the insurance company to their clients against payment of insurance premium.

The insurance industry should continue to develop products that meet the fast evolving risks while the organizations of all sizes must hinder the warnings and take steps to mitigate cyber risks in the same manner that they have grown used to deal with operational, regulatory and other risk inherent in their way of doing business in local or international market.

Nowadays insuring against Cyber risks offered by several insurance markets around the world offering the cover to their potential clients who include protection against costs arising from information leakage, and most of insurers cater more toward business policies rather than personal policies.

There are several challenges related to cyber insurance such as the assessment of cyber security and cyber risk in terms of monetary costs and benefits, managing of cyber insurance portfolio.

There are also future threats and trends due to Cyber risk environment continuously changes have to be monitored and observed for underwriting this type of business.

**Therefore the cyber insurance need for reliable method, tools and for their management process and offering the best products suited with the client's needs.**

**In general the following parts will be discussed in this chapter as follows:**

**Part 1: Cyber Insurance;** this part will introduce the definition of cyber insurance, history of cyber insurance, Insurance Policy structure include scope of cover , exclusions and uninsurable cyber risks as well as the cyber insurance carriers and underwriting this type of business

**Part 2: Cyber Insurance Market ,** this part will introduce the features of the cyber insurance global market, challenges and opportunities of underwriting this type of business, support the market through regulations, the cyber risk position per industry and products suitable for them as well as the future of cyber insurance.

## Part 1

### Cyber Insurance

In this part we will discuss the definition of cyber insurance, history of cyber insurance, Insurance Policy structure include scope of cover , exclusions and uninsurable cyber risks as well as the cyber insurance carriers and underwriting this type of business

#### **1. Definition of Cyber Insurance:**

Cyber insurance is an insurance product used to protect businesses and individual users from Internet-based risks and more generally from risks relating to information technology infrastructure and activities against financial loss. Risks of this nature are typically excluded from traditional commercial general liability policies while some existing insurance policies such as commercial property, business interruption or professional indemnity insurance may provide some elements of cover against cyber risks, businesses are increasingly buying specialized cyber insurance policies to supplement their existing insurance arrangements, coverage provided by cyber-insurance policies may include first-party coverage against losses such as data destruction, extortion, theft, hacking, denial of service attacks and liability coverage indemnifying companies for losses to others caused for example, by errors and omissions, failure to safeguard data, or defamation and other benefits including regular security-audit, post-incident public relations and investigative expenses, and criminal reward funds. However some risks are uninsurable because the potential costs are impossible to evaluate; these include reputation damage, loss of trust from stakeholders such as regulators and lowered employee morale.

#### **2. The overview of cyber insurance product<sup>26</sup>:**

Due to the cyber-insurance market in many countries is relatively small compared to other insurance products its overall impact on emerging cyber threats is difficult to quantify and the impact to people and businesses from cyber threats is also relatively broad when compared to the scope of protection provided by insurance products, insurance companies develop and change insurance products to be increasingly purchased. The underwriting criteria for insurers to offer cyber-insurance products are also early in development, and underwriters are actively partnering with IT security companies to develop their products as well as directly improving security, cyber-insurance is enormously beneficial in the event of a large-scale security breach. Finally Insurance allows cyber-security risks to be distributed fairly with cost of premiums commensurate with the size of expected loss from such risks.

#### **3. History of the development in Cyber Insurance and its regulations :**

There are differences between the cyber insurance in the US , Europe and Asia and each market has its features, development and underwriting but in this case study we will discuss deeply the European market development , regulations and underwriting due to the European market is an open market which their capabilities and capacity through Lloyd's syndicates or London market are available to all

---

<sup>26</sup> Martin Eling and JingjingZhu ;"Which Insurers Write Cyber Insurance? Evidence from the U.S. Property and Casualty Insurance Industry", e article, *Journal of Insurance Issues*, 2018, 41 (1): 22-56.



insurers around the world which making study their experience available for the remaining markets to benefit from their expertise although US insurance market is more advanced than its counterparts in Europe and Asia. In respect of the US market In the late 90's the first policies written to address this exposure were written to address online content or software in their basic coverage's and in the early 2000's the online media policies started to cover unauthorized access, network security", and virus related claims, in the Mid 2000's polices evolved to add some 1st party coverage's these would include Cyber Business Interruption, Cyber Extortion, and Network Asset Damage. The California Security Breach and Information Act became 2003 it had a real effect on exposure and insurance, in the late 2000's many of the coverage's being offered were only available with a small sub-limit and In 2016 products and appetite continue to evolve as well as the services that come with the policy<sup>27</sup>.

In respect of the European market it works in the 1990s through the cover which is tightly limited approached to different clients including SME's and establish data protection as right for EU citizen then it had developed by the Lloyd's of London market in 2000 to provide the first and third-party coverage as well as the business interruption coverage while such errors & omissions have likely happened, suits against organizations on this basis have proven to be rare in the light of existing high profile and hacking scandals<sup>28</sup>.

The focus of forms that have developed since 2000 has been on business interruption, payment of fines and penalties, credit monitoring costs, public relations costs and the cost of restoring or rebuilding private data and they continue to expand and evolve today based on the EU announced the cyber security directive which impose the security measures on business in addition, technology errors & omissions policies are now sold with third-party coverage to organizations, such as programmers and technology installers who could get sued if their advice or product fails to be satisfactory to their clients<sup>29</sup>, then in 2015 the EU implemented the reform of the data protecting legislation which impose introduces a common data breach notification requirement that all companies worldwide that process personal data of EU citizens which the enforcement is also backed by significant fines of up to €20m or 4% of group annual global turnover requires organizations to notify the local data protection authority of a data breach within 72 hours of discovering it which means organizations need to ensure they have the technologies and processes in place that will enable them to detect and respond to a data breach<sup>30</sup>.

<sup>27</sup> Prowriters ;"The History of Cyber Insurance", Website Article, Published on 25th April 2016, Available from <http://prowritersins.com/the-history-of-cyber-insurance/> (Accessed 23rd July 2018).

<sup>28</sup> gc capital ideas; "Historical Development Of Cyber (Re)Insurance", Website Article , Published on 23rd October 2014 ,Available from <http://www.gccapitalideas.com/2014/10/23/historical-development-of-cyber-reinsurance/>(Accessed 23rd July 2018).

<sup>29</sup> Xprimm , "The EU cyber insurance market in the run-up to GDPR implementation", Website Article, Published on 26th April 2018, Available from <http://www.xprimm.com/The-EU-cyber-insurance-market-in-the-run-up-to-GDPR-implementation-articol-117,149-11121.htm>(Accessed 23rd July 2018).

<sup>30</sup> Kris Lahiri , "What Is General Data Protection Regulation? "Website Article Published on 14th February 2018, Available from <https://www.forbes.com/sites/quora/2018/02/14/what-is-general-data-protection-regulation/> (Accessed 23rd July 2018).

#### 4. The gaps in the market that cyber insurance fills it:

A cyber insurance policy is designed to compensate business losses from the impact of a cyber-breach including data loss, business interruption, and network damage. This type of insurance requires certain IT controls and quality preventative measures in order for basic eligibility it will be often reflect to reduce insurance premiums and the option for higher liability coverage limits. Cyber liability policies typically cover a variety of both liability and property losses when a business experiences a data breach. Network cyber security and privacy policies address the organization's liability for a data breach in which customer personal information is exposed or stolen by unauthorized access to the organization's network. The range of covered expenses associated with data breaches can include notification costs, credit monitoring services for customers, legal costs to defend claims by state regulators, other fines and penalties, and losses resulting from customer identity theft.

All these damages consider valuable opportunity to insurance underwriter who can offer specialist expertise in data security and can alert clients in real time to attacks. The both industrial and service sectors integrate their entire production systems into complex software systems, hackers will not be able to access data they will be able to disrupt production it may be result to terrorist attacks.

#### 5. Cyber Insurance Product :

Despite the continuous development of the defense methodologies and increasing recognition by organization of the need to put in place adequate cyber risk management systems and controls, there are a number of sophisticated attacks may not be prevented or even preventable .Cyber insurance therefore is the best solution to mitigate this type of risk in the same manner as other risk to which both risk managers and the insurance industry are more accustomed to addressing which is considered second line of defense risk management tool .

When assessing whether an insurance policy covers cyber risks, its coverage should be looked at mainly from two angles scope and trigger which mean the basic scope of cover provided by the policy and its extensions to extend the cover to include several covers under the whole cover of the policy coverage.

##### 5.1. The Scope Of Cover<sup>31</sup> :

There are a variety of specialist cyber insurance products are available which products can be tailored to the need of the specific clients and the global cover is available, the underwriters become more responsive to the demand side requirements and the changing technological and regulatory landscape as well as vary the policy wording depending on the market and jurisdiction, the scope of cover include the following sections as below:

---

<sup>31</sup> Lloyd's, "Cyber products at Lloyd's", website article, Available from <https://www.lloyds.com/about-lloyds/what-lloyds-insures/cyber/cyber-products/> (Accessed 26rd July 2018)

**5.1.1.1. Data Protection Breaches and Third Party Liability :**

Under this section the insurer will pay for losses incurred by client if he suffer from the unauthorized access and use or disclosure of personal data including (the costs of outside computer forensic analysis to confirm the breach; legal costs incurred in managing the breach; costs incurred in notifying data subjects and any regulatory body, credit monitoring costs where required) as well as payment for the incurred loss to suppliers due to failure of the client's control to include the defense and indemnity costs

**5.1.1.2. Network Damage:**

The cover under this section include the payment by the insurer the remediation costs of damages relating to the theft of hardware which include relevant information, data contamination due to a virus or data leak in respect of intentional or unintentional actions of an employee .

**5.1.1.3. Cyber business interruption:**

The payment of compensation by the underwriter if the client's business suffer from an interruption as a result of a cyber-attack from a third-party or a hacker will include the following (loss of income including and increased cost of working as well as the reputational harm which extend for financial losses incurred from loss of contracts due to a cyber-incident.

**5.1.1.4. Hacker damage:**

The cover under this section includes the payment by the insurer for the losses caused by damage or corruption; copying or stealing of programs or data held electronically.

**5.1.1.5. Cyber extortion:**

This section include the payment cost of investigation into the case of threat if the insured had received a threat from a third-party to damage the computer systems or disseminate commercially sensitive information, the payment compensation will include the cost of any ransom demand and value of any good or services surrendered.

**5.1.1.6. Privacy protection/ Regulatory :**

If a claim is made against the client for breach of personal data or sensitive commercial information, the compensation payment will extend to include the amount of any regulatory award against client where legally insurable; the costs incurred in defending a regulatory investigation or prosecution and the costs of outside computer forensic analysis to confirm the breach.

**5.1.1.7. Media liability**

Under this section the insurer will pay a claim made against the client arising from the content email, website or other electronic communications as a result of alterations made by a hacker, the section will indemnify the client for infringement of intellectual property rights ,defamation and negligent transmission of a virus.

## 5.2. The Cyber Policies Exclusions and Limitations<sup>32</sup>:

Each type of policies have its general exclusions which mentioned in the policy wording that include provisions that eliminate coverage as well as exclude the compensation for specific perils as follows:

### 5.2.1.1. Claims, losses, breaches, privacy investigations:

This exclusion clarify that there is no payment under the policy in respect of claims, losses, breaches, privacy investigations as well as threats due to provision of professional advice or services, failure of an internet service provider, breach of intellectual property rights other than under the media liability section in case of it especially mentioned in the cover, injury or damage to tangible property, reasonably to have known about before the policy started and any acts or omissions that the client deliberately or recklessly commit.

### 5.2.1.2. Limitation on the compensation claim amount:

The payment of any payable claim will be reduced in case of the insurer restricted their rights of recovery against a third-party do admit by the client to liable for third party without prior written agreement from the insurer.

## 5.3. The Cyber Policy Holder obligations in case of cyber claim:

Making a claim for cyber insurance is no different to the process of claiming for most insurance types, although it's likely the claim amount is higher than traditional policies which will mean the process can take longer time .Like all insurance claims the client have to fill out a claims form though the underwriter website to fill the personal and business information, description of the incident, the products or costs liable ,property or people damaged and whether there were any witnesses to the event. Following this the underwriter will be processed to further steps to process the claim.

## 6. The Cyber Insurance underwriters in the global market:

Choosing between different cyber insurance underwriters can be tough to connect by the client with a underwriter who best fits the needs and have enough expertise in this line of business. The following are the top five cyber insurance underwriters in the market producing whose taking initiative to innovative and approaches providing this type of cover:

### 6.1. AIG<sup>33</sup>

---

<sup>32</sup> Hiscox, "What is cyber and data risks insurance?", Cyber and data policy wording, Available from <https://www.hiscox.co.uk/sites/uk/files/documents/2017-03/13388-cyber-and-data-policy-wording.pdf> (Accessed 26th July 2018)

<sup>33</sup> Jayleen R. Heft , "Top 10 writers of cyber security insurance", website article, published on 13th November 2017, Available from <https://www.propertycasualty360.com/2017/11/13/top-10-writers-of-cybersecurity-insurance/> (Accessed 26th July 2018)

American International group aims to provide an end-to-end approach to supporting customers with cyber insurance needs, providing loss prevention tools and services geared toward regaining stability following a data breach. AIG market share 22 per cent of the whole global cyber insurance market and is the first one underwriter of the earliest to have taken step to create and innovative cyber insurance product.

## 6.2. Hiscox

Hiscox is coming in at No. 2 for their global market share, a Bermuda-incorporated insurance. Hiscox's cyber policy available for corporate and personal business it covers privacy, data breaches, network exposures and instances of human failure in the form of employee negligence. Hiscox also makes the valuable point that cyber security should be a top priority for all sizes of business, reinstating the fact that no one can guarantee definite safety from hackers – a prime reason for cyber insurance.

## 6.3. Marsh

Marsh is Global insurance broker and risk adviser, Marsh is taking the approach of analyzing how well a customer is managing the risk through the quantitative assessment uses statistical models that are then applied to the underwriting process.

## 6.4. Lloyd's of London<sup>34</sup>

Lloyd's makes it clear that technology, and cyber more specifically, has created an entirely new insurance frontier through the approach had been taken to look beyond the protection of finances by also providing a consultancy capacity up to £500 Million. Lloyd's boasts access to 77 expert cyber risk insurers from a single point that's able to tailored cyber insurance policies to suit individual customers and their own specific risk landscape.

## 6.5. Willis Towers Watson

Willis Towers Watson aims to add value for customers purchasing cyber insurance by providing access to specialist knowledge, 'off the shelf'<sup>35</sup> solutions and extensive experience in handling these claims comparable to the Lloyd's approach.

## 7. Management and Underwriting of Cyber Risks:

Almost of the cyber insurance underwriters implement their own standard risk assessment and coverage elements while underwriting this type of business and due to the sensitivity of the information clients are often reluctant to share details of their security measures and history of incidents through the underwriting questionnaire or model to the insurers as this will help the underwriter while

---

<sup>34</sup> Lloyd's, "Cyber Risk. Cyber Secure", YouTube video, Available from <https://www.lloyds.com/about-lloyds/what-lloyds-insures/cyber> (Accessed 27th July 2018)

<sup>35</sup> TOM BALL REPORTER, "Top 5 cyber insurance providers offering the best cover against attack", website article, published on 30th January 2018, Available from <https://www.cbronline.com/list/top-5-cyber-insurance-providers> (Accessed 27th July 2018)

underwriting and reinsurance process , the insurers building also a team of Cyber Risk Consultants to assist for the underwriting, evaluate and determine the highest impact , loss prevention process and continuously improving the cyber risk posture over the policy period. Therefore the insurers prior issuance this type of policies have to set their executing strategic priorities such as earning stabilization and increase of earnings power focus on profitability ,business development , building new business model and complexity reduction. In order to achieve these objectives the insurers have to follow the below steps in order to manage well the cyber insurance portfolio<sup>36</sup>:

#### **7.1. Check the insured security and business continuity plan:**

The insurers and reinsurers have to check the insured security through Threat analysis which include critical systems structure and data analysis, the Cloud systems and outsourcing mechanism, Operational risk scenario analysis, Risk awareness and Crisis management. As well as the business continuity plan in case of such cyber incident including the client response to recover and eliminate the impact of such breach.

#### **7.2. Set Up The Cyber Insurance Scheme of underwriting:**

The insurers have to setup the policy wording which includes the cover, conditions and exclusions.as well as arrange to best method of reinsurance capacity based on the size of business and expertise of the underwriter in this type of business, perform cyber risk assessment standards, recruit of professional consultant, setoff pricing scale and build a team of claims experts<sup>37</sup>.

#### **7.3. Underwriting and portfolio management**

After the insurers had finalize the reinsurance treaty or suitable method and create the policies wording the insurers had to setup their underwriting guidelines including their exclusion clauses based on the agreements with reinsurers ,creation of cyber loss scenarios and how to act ,loss monitoring strategy ,product development and the best way to manage different types accumulation exposures which range from Self-reproducing computer viruses to Global Outage<sup>38</sup> of the Internet which need the regular monitor and quick response.

#### **7.4. The Compliance Procedures:**

Finally the insurers have to setup the compliance procedures of the best practice cyber insurance underwriting including fully commitment service level agreements with different business partners, Legal protection and contractual penalties.

---

<sup>36</sup> Aon Risk Solutions, *Global Risk Management Survey 2017,Annual Report*, Available from <http://www.aon.com/2017-global-risk-management-survey/pdfs/2017-Aon-Global-Risk-Management-Survey-Full-Report-062617.pdf>/(Accessed 27th July 2018)

<sup>37</sup> KELLY, BILLI,"4 Keys to Bridging the Cyber Insurance Gap." *Article, Claims*. Oct2017, Vol. 65 Issue 10, p22-24. 3p.

<sup>38</sup> Heidi A. Strauß,"Cyber Risks(Threats – Trends – Mitigation)",*Training presentation,2018 Münchener Rückversicherungs-Gesellschaft,Munich 12nd June 2018 Page 25-34*

## Part 2

### Cyber Insurance Industry

In this part we will discuss the features of the cyber insurance industry including their global market, opportunities and challenges of underwriting this type of business, support the market through regulations, the cyber risk position per industry and products suitable for them as well as the future of cyber insurance.

#### **1. Features of the Cyber insurance global market:**

The insurance market including insurers reinsurers, brokers and relevant associations whose have an important role to play in providing greater clarity about the coverage available for cyber risk and which policies provide that coverage. Different approaches of coverage provided by different underwriters allow for innovation and availability for several options to clients however differences in terminology and diverging approaches to offering coverage exacerbate an already significant amount of misunderstanding among clients on how to protect against themselves from the financial impacts of cyber risks. Cyber Insurance is a volatile market and is growing at over 30% annually so it is a useful source of new revenue the advantage to insurers of being able to convince clients to aloe real-time integration of the client's telematics systems with the insurer's security alert systems.

The GWP of global cyber insurance market could grow to USD 5 billion in annual premiums by 2018 and at least USD 7.5 billion by the end of the decade, according to a new report issued by PwC.<sup>39</sup>

The cyber insurance market is categorized on the basis of enterprise size, service, and industry. Large enterprises led the cyber insurance market in terms of size, due to their high purchasing power and the availability of sufficient funds for risk insurance. Since the premiums for cyber insurance are very high, SMEs refrain to buy expensive covers because of their limited budget constrains over cyber risk management. Among all the industries, banking financial services and insurance (BFSI) had been the largest consumer for cyber insurance market as these companies are more prone to cyber-attacks ,this industry contributed more than 35% of the global market share in 2016<sup>40</sup>. The market will be witnessing the fastest growth in retail and manufacturing industries, during the forecast period, due to numerous cyber challenges and risks present in the industry, such as digital supply chain management and online operations<sup>41</sup>.

---

<sup>39</sup> Daniela GHETU, "PwC: Cyber insurance market set to reach USD 7.5 billion by 2020", Websire Article ,Published on 28th September 2017, Available from <http://www.xprimm.com/PwC-Cyber-insurance-market-set-to-reach-USD-7-5-billion-by-2020-articol-117,124-9981.htm>(Accessed 28th July 2018)

<sup>40</sup> Aon Risk Solutions, Global Risk Management Survey 2017, Annual Report, Available from <http://www.aon.com/2017-global-risk-management-survey/pdfs/2017-Aon-Global-Risk-Management-Survey-Full-Report-062617.pdf>/(Accessed 27th July 2018)

<sup>41</sup> Allied Market Research, "Cyber Insurance Market to Reach \$14 Billion, Globally, by 2022"., Website Article , Available from <https://www.alliedmarketresearch.com/press-release/cyber-insurance-market.html>(Accessed 28th July 2018)

The increasing interconnectivity, commercialization, and globalization of cybercrime are driving greater frequency and severity of cyber incidents, including past data breach incidents which impacted the growth of the cyber insurance market positively and had led to increase in the demand for cyber liabilities and sophisticated policy cover by business leaders, to protect the enterprise data from cyber-attacks and cyber risks. The global cyber insurance industry is moderately competitive with players developing new strategies to reach their customers in the most effective and efficient way through the underwriters which mentioned before in the previous part of this chapter.

## **2. Cyber insurance opportunities and challenges:**

Insurance Markets will increasingly be confronted with emerging cyber risks, therefore insurers who willing to provide their clients with ease of mind by balancing expert services on risk mitigation with limiting impact through fast incident response and solid after-care and these process can be done by development of cyber risk transfer capabilities which require integrating the various perspectives of markets, business, technology, innovation, and cyber security and this requires organizational and cultural change which is considered great opportunity to prepare the company to get ready for this innovation through implementing several steps include<sup>42</sup>(enhance own cyber risk management capabilities to stay ahead of evolving threats, comply with new regulations and use its knowledge and insight for product development, deepen client engagement through joint development of cyber risk transfer products that fit the increasingly digital world and that differentiate themselves through ancillary services, collaborate with other insurers on market and cyber security firms for the benefit of all clients, develop cyber insurance products on a small scale)in order to achieve the growth for the portfolio of cyber insurance which is consider opportunity to the insurers to expand their business.

On the other side the cyber industry include several challenges in underwriting and management portfolio of this type of business include<sup>43</sup> (limited availability of historical data to allow for accurate pricing of insurance premiums which led to insurers have entered into partnerships with information technology security firms to improve their access to information on incidents, accumulation risk as all the software are common and used by all clients so the insurers can pass this challenges by building a large pool of diversified risks among themselves, reinsurance availability and lack of awareness of potential cyber losses ).All theses challenges require from the underwriters in the cyber insurance market to find solutions or innovate approaches to addressing the challenges to understanding cyber insurance coverage , supporting greater market capacity and managing of accumulation risks.

## **3. Cyber-security regulation/Data Protection for the Insurance Sector :**

A new cyber security regulation comprises directives that safeguard information technology and computer systems with the purpose of forcing companies and organizations to protect their systems and

---

<sup>42</sup> Marano, Pierpaolo-Rokas, Iōannēs- Kochenburger, Peter ; "The 'Dematerialized' Insurance : Distance Selling and Cyber Risks From an International Perspective", eBook., Switzerland : Springer. 2016, Pages 186-193

<sup>43</sup> OECD , "Enhancing the role of insurance in cyber risk management", Report, Date of publication 8 December 2017, Available from <https://www.oecd.org/daf/fin/insurance/Enhancing-the-Role-of-Insurance-in-Cyber-Risk-Management.pdf> pages from 95-136



information from cyber-attacks, there are numerous measures available to prevent cyber-attacks through follow cyber security measures include firewalls, anti-virus software and prevention systems. There have been attempts to improve cyber security through regulation and collaborative efforts between government and the private sector to encourage voluntary improvements to enhance cyber security standards in order to eliminate such losses.

Nowadays there are existing cyber-security regulation cover different aspects of business operations differ from country's society, infrastructure and values as in the United States of America there are three regulations 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act and one Proposed regulation The Consumer Data Security and Notification Act amends the Gramm-Leach-Bliley Act<sup>44</sup>, and in the European Union had created a more tailored regulation for businesses operating specifically within the EU through three major regulations within the EU include ENISA The European Union Agency for Network and Information Security, NIS Directive<sup>45</sup> and EU General Data Protection Regulation(GDPR)

EU General Data Protection Regulation (GDPR) <sup>46</sup>was enforcement 25 May 2018 to bring a single standard for data protection among all member states in the EU. It applies to entities that operate in the EU or deal with the data of any resident of the EU regardless of where the data is processed as we discussed in the previous chapter.

#### 4. Ranking of Cyber Risk Position Per Industry:

According to the Aon Risk Solutions Annual Report Global Risk Management Survey 2017 the Cybercrime/hacking/viruses/malicious codes ranks number five of the top ten risks in the global insurance market in 2017 and expected to be the same rank in 2020.It also rank number one of the risks by region in North America in 2017

In response to this now emergent threat more companies are either adopting cyber risk assessments (53 percent), transferring greater risk to the commercial insurance market (33 percent), or evaluating alternative risk transfer measures (captive use is projected to rise from 12 percent to 23 percent by 2020).

However, only 23 percent of companies currently employ any financial quantification within the cyber risk assessment process. Without the financial stats, risk managers will find it hard to adequately prioritize capital investment in risk mitigation, or attract sufficient attention from a potentially less tech-proficient board.

About 33 percent of surveyed companies are now purchasing cyber coverage, up from 21 percent in the previous survey. Regionally, this uptake remains inconsistent. North American companies lead the

<sup>44</sup> appknox,"A Glance At The United States Cyber Security Laws", website Article, Available from <https://blog.appknox.com/a-glance-at-the-united-states-cyber-security-laws/>(Accessed 27th July 2018)

<sup>45</sup> Carter Schoenberg, "Cyber insurance in the 2018 regulatory landscape", Website Article , Published on 16th January 2018,Available from <https://www.csoonline.com/article/3247834/risk-management/cyber-insurance-in-the-2018-regulatory-landscape.html>(Accessed 28 July 2018)

<sup>46</sup> Marano, Pierpaolo-Rokas, Iōannēs- Kochenburger, Peter ; "The 'Dematerialized' Insurance : Distance Selling and Cyber Risks From an International Perspective", eBook., Switzerland : Springer. 2016, Pages 225-230

regions in purchasing cyber coverage (68 percent) while those in Latin America remain way behind at nine percent.

The below schedule contain the huge industries in the global economy and the ranking of top three risks that they exposed during their operational process:

Industry	Key Risk 1	Key Risk 2	Key Risk 3
Agribusiness	Commodity price risk	Weather/natural disasters	Increasing competition
Aviation	Workforce shortage	Increasing competition	Cybercrime/hacking/ viruses/malicious codes
Banks	Regulatory/legislative changes	Cybercrime/hacking/ viruses/malicious codes	Damage to reputation/brand
Beverages	Damage to reputation/brand	Economic slowdown/slow recovery	Commodity price risk
Chemicals	Increasing competition	Economic slowdown/slow recovery	Commodity price risk
Conglomerate	Economic slowdown/slow recovery	Increasing competition	Major project failure
Construction	Economic slowdown/slow recovery	Increasing competition	Workforce shortage
Consumer Goods Manufacturing	Economic slowdown/slow recovery	Increasing competition	Failure to innovate/meet customer needs
Education	Cybercrime/hacking/ viruses/malicious codes	Damage to reputation/brand	Regulatory/legislative changes
Energy (Oil, Gas, Mining, Natural Resources)	Commodity price risk	Regulatory/legislative changes	Economic slowdown/slow recovery
Food Processing and Distribution	Damage to reputation/brand	Failure to innovate/meet customer needs	Commodity price risk
Government	Damage to reputation/brand	Cybercrime/hacking/ viruses/malicious codes	Failure to attract or retain top talent
Health Care	Regulatory/legislative changes	Cybercrime/hacking/ viruses/malicious codes	Failure to innovate/meet customer need

Hotels and Hospitality	Economic slowdown/slow recovery	Cybercrime/hacking/viruses/malicious codes	Political risk/uncertainties
Insurance, Investment and Finance	Failure to innovate/meet customer needs	Regulatory/legislative changes	Cybercrime/hacking/viruses/malicious codes
Life Sciences	Regulatory/legislative changes	Merger/acquisition/restructuring	Failure to innovate/meet customer needs
Lumber, Furniture, Paper and Packaging	Economic slowdown/slow recovery	Commodity price risk	Political risk/uncertainties
Machinery and Equipment Manufacturers	Economic slowdown/slow recovery	Increasing competition	Globalization/emerging markets
Metal Milling and Manufacturing	Economic slowdown/slow recovery	Commodity price risk	Increasing competition
Non-Aviation Transportation Manufacturing	Economic slowdown/slow recovery	Failure to innovate/meet customer needs	Product recall
Non-Aviation Transportation Services	Increasing competition	Economic slowdown/slow recovery	Failure to innovate/meet customer needs
Nonprofits	Political risk/uncertainties	Failure to innovate/meet customer needs	Regulatory/legislative changes
Power/Utilities	Regulatory/legislative changes	Cybercrime/hacking/viruses/malicious codes	Major project failure
Printing and Publishing	Failure to innovate/meet customer needs	Failure to attract or retain top talent	Cash flow/liquidity risk
Professional and Personal Services	Economic slowdown/slow recovery	Failure to attract or retain top talent	Damage to reputation/brand
Real Estate	Economic slowdown/slow recovery	Property damage	Failure to innovate/meet customer needs
Restaurants	Economic slowdown/slow recovery	Damage to reputation/brand	Workforce shortage
Retail Trade	Economic slowdown/slow recovery	Increasing competition	Failure to innovate/meet customer needs
Rubber, Plastics, Stone and Cement	Economic slowdown/slow recovery	Increasing competition	Failure to innovate/meet customer needs

Technology	Failure to innovate/meet customer needs	Disruptive technologies/innovation	Failure to attract or retain top talent
Telecommunications and Broadcasting	Failure to innovate/meet customer needs	Increasing competition	Disruptive technologies/innovation
Textiles	Economic slowdown/slow recovery	Increasing competition	Failure to innovate/meet customer needs
Wholesale Trade	Increasing competition	Economic slowdown/slow recovery	Commodity price risk

*[Source: Aon Risk Solutions, Global Risk Management Survey 2017, Annual Report, Available from <http://www.aon.com/2017-global-risk-management-survey/pdfs/2017-Aon-Global-Risk-Management-Survey-Full-Report-062617.pdf/> (Accessed 27th July 2018)]*

It shown from the previous schedule for the top three risks belong to almost industries has valuable effect on the global economy that the Cybercrime/hacking/viruses/malicious codes consider critical threat for specific highlighted industries like Aviation, Banks, Education, Government, Health Care, Hotels and Hospitality, Insurance, Investment and Finance and finally Power/Utilities sectors.it shown also that the majority of paid claims as result of cyber breach belong to the above sector with especially silent cyber risk which need different treatment and assistance form the insures side .

**5. Cyber Insurance Underwriting and Products Suitable To Different Industries :**

Although there is an existing standard Cyber Policy available through the underwriters and reinsurers whose underwrite or sharing this type of risk, there are a variety of specialist cyber insurance products are available which products can be tailored to the need of the specific clients and the global cover is available, the underwriters become more responsive to the demand side requirements and the changing technological and regulatory landscape as well as vary the policy wording depending on the market and jurisdiction as there is many forms to be standalone policy or separate section under package policy or extension under property all risks policy with specified minor applicable limit.

Here are the cyber insurance products belong to several industries as follows:

**5.1. Aviation Sector :**

Aviation industry is increasingly reliant on the efficiencies of IT infrastructure and the data stored therein<sup>47</sup>, therefore cyber risks are considerable effect on their financial impact like affecting online ticketing services. The need for obtain tailored coverage at agreed-upon terms standalone policy or under the Aviation package all risks policy which extend to<sup>48</sup> cover the data breach response, forensic costs, Losses stemming from social engineering schemes, including fraudulent money transfers and

*47 Juliann Walsh, "Protecting 'Flying Computers' "website article ,published on 5th July 2016,Availabe from <http://riskandinsurance.com/cyber-risk-aviation/>(Accessed 28th July 2018)*

*48 Insurance Journal, "Willis Towers Watson Adds Cyber Coverage to Aviation Offering", Website Article, Published on 28th February 2018,Available from <https://www.insurancejournal.com/news/national/2018/02/28/481763.htm>(Accessed 28th July 2018)*

business interruption losses following a data-security event targeting the clients computer system as well as third party liability. In addition this industry is moderate when evaluate their general risk profile

### **5.2. Financial Sector like Banks, Insurance, Investment and Finance:**

Among all the industries banking financial services and insurance (BFSI) had been the largest consumer for cyber insurance market as these companies are more prone to cyber-attack. This sector has tailored package policy Bankers Blanket Bond (BBB)<sup>49</sup> which extend the cover to include Professional Indemnity, Directors and Officers and Computer and cyber fraud as well as fraudulent electronic funds payments the cyber-attacks, forensic investigation, business interruption, extortion and Computer data loss and restoration will be suitable products to this industry whether the policy issued on standalone basis or package BBB policy In addition this industry is moderate when evaluate their general risk profile due to the precautions had been taken by the management of this sector .

### **5.3. Education Sector:**

As shown in the previous schedule of the top three risks that the Cybercrime/hacking/viruses/malicious codes in the rank number one due to the nature of their operations and several time of been encrypted the student and staff records as well as the educational institutions are increasingly embracing outsourcing for internet usage and social networking. Therefore there is specific need to cover these risks through standalone policy or tailored package policy property or liability to include the cover of investigation and hiring of a public relations or marketing firm to help manage the educational firm response to an attack, credit monitoring for students and staff whose records have been exposed, Legal support and business interruption. The education sector has to apply for the proposed adjustments received from the insurer in order to enhance the risk profile due to their classification of critical businesses.

### **5.4. Government Sector:**

The Cybercrime/hacking/viruses/malicious codes for the governments ranking the number two as per shown in the previous schedule of the top three risks due to that the government networks and critical infrastructure around the world are under a consistent state of attack. However the nature of the threats is anything but constant, the attacks evolve on a daily basis as hacktivists, nation states and cyber criminals. Therefore there is specific need to cover these risks through standalone policy include the cover of the threats or arrange an appropriate insurance program in order to combating cyber Crime as well as apply for the proposed adjustments received from the insurer in order to enhance the risk profile. The cover have to include forensic investigation expenses, crisis management and public relations expenses, asset replacement, response costs to rectify harm, business interruption, legal defense costs and compensation to third parties like the case of<sup>50</sup> Queensland Government agencies are

---

<sup>49</sup> Taplin, Ruth, "Managing Cyber Risk in the Financial Sector: Lessons From Asia, Europe and the SA", E Book, London : Routledge. 2016, Pages 63-69

<sup>50</sup> Queensland Government, "Cyber security insurance for Queensland Government agencies", Official Article ,last Reviewed 20th December 2017, Availabel from <https://www.qgcio.qld.gov.au/documents/cybersecurity-insurance-for-queensland-government-agencies>(Accessed29th July 2018)

automatically covered by the Queensland Government Insurance Fund(QGIF) in the event of a cyber-security incident.

#### **5.5. Health Care Sector:**

Due to the threat of stolen health records is considered more valuable than stolen credit card as well as the ranking of cyber risk is number two the cyber insurance cover is critical for the health care sector due to their work nature of complex chain of liability from providers, third party administrators, outsourced network service providers and data storage firms and Sharing of health information with a variety of providers. Therefore there is specific need to cover these risks through standalone policy or tailored package policy property or liability to include the cover general Liability for bodily injury and property damage belong to third party, Errors & Omissions and Crime. The cyber insurance can be used to pay HIPAA fines as per Health Insurance Portability & Accountability Act (HIPAA) and the Health Information Technology for Economics & Clinical Health Act (HITECH) and other costs associated with data breaches<sup>51</sup>.

#### **5.6. Hotels and Hospitality Sector :**

Due to the high degree of dependency on electronic processes or computer networks vendors and independent contractors or additional service providers which ked the cyber-crime risk became the number two of top three risks in this sector, therefore the Cyber insurance is a relatively growing to cover these risks through standalone policy or tailored package policy property or liability to include the cyber coverage sections. In addition this industry is may differ while evaluating their general risk profile

#### **5.7. Power/Utilities sector:**

The Power/Utilities and Energy sector is essentially rely on operate critical infrastructure, potentially large amounts of customer and employee data, dynamic regulatory environment and bodily injury or property damage may resulting from cyber incident , therefore there is specific need to cover these risks through standalone policy or tailored package policy property or liability to include the cover general Liability for bodily injury and property damage belong to third party, Errors & Omissions and Crime including security or privacy breach regulatory proceedings fines and penalties within the scope of cover and apply any adjustments proposed by the insurer due to the sector classification of critical businesses.

#### **5.8. Supply Chain Sector<sup>52</sup>:**

Due to the supply chain nature of work on cyber resilience through dealing with different risks touch sourcing, vendor management, supply chain continuity and quality, transportation security and many other functions across the enterprise and require a coordinated effort to address. It shown when third-party supplier provides technology to the company or is connected to the company's systems, then the

---

*51 Allison Berke,"15 Days of Cyber Insurance: Is cyber insurance health insurance?", Website article ,Stanford University ,Available from <https://cyber.stanford.edu/15-days-cyber-insurance-cyber-insurance-health-insurance>(Accessed29th July 2018)*

*52 Manners-Bell, John , "Supply Chain Risk : Understanding Emerging Threats to Global Supply Chains", EBook, London : Kogan Page. 2014,Pages 222-225*

company faces cyber incident or crime. In fact there are many examples of companies' supply chains being hacked via a third-party supplier or a business partner which led that the companies need to take a closer look at who they are connecting to on the data side. Therefore cyber insurance in the supply chain cannot be viewed as an IT problem only it extend to cover third party, poor information security practices and software security vulnerabilities in supply chain management or supplier systems in respect of logistics networking.

### 5.9. Petrochemicals Sector :

The Petrochemicals industry processed their work through Industrial Control Systems (ICS), which comprises all necessary hardware and software to control and monitor process equipment in respect of operational and information technology which include Supervisory Control and Data Acquisitions Systems (SCADA) and Distributed Control Systems (DCS)<sup>53</sup>. Due to interconnectivity a cybercrime to a plant could come via a business system to which it is connected for information transfer purposes. Therefore the nature of work shall be taken into consideration while evaluate the risk profile of the clients as well as the types of control systems used in their industrial process control for production and manufacturing purposes. All these scenarios and process of nature of work of this sector reflect a specific need to cover these risks through standalone policy include the cover of the threats or arrange an appropriate insurance program in order to combating cyber Crime as well as apply for the proposed adjustments received from the insurer in order to enhance the risk profile. The cover has to arrange to include all sections previously discussed before.

### 6. The Future of Cyber Insurance Market:

Cyber insurance is a potentially huge and businesses across all sectors are beginning to recognize the importance of cyber insurance with the increasingly complex and high risk digital landscape. It considered real opportunity to gain more much premiums from the prospective of insurers as well as the clients will secure from cyber risks. The cyber insurance could soon become a client expectation and insurers that are unwilling to embrace it risk losing out on other business if cyber products don't form part of their offering. In the meantime, many insurers face considerable cyber exposures for management their portfolios due to connected critical infrastructure, development of digital systems ,IT companies gain monopolistic power of information like Google, Amazon, Facebook, Apple and New kinds of cyber risks emerge unexpectedly and develop fast . Therefore the insurers have to arrange suitable reinsurance technique and taken the precautions to protect their portfolios as well as improve the information available for underwriting and for determining aggregation risk.

---

<sup>53</sup> 53 John Munnings-Tomes & Jonathan Scott, "Cyber Security & Safety Considerations For Oil, Gas & Petrochemical Risk Assessment", Report belong to Lma Lloyd's , Available from <http://www.lmalloyds.com/AsiCommon/Controls/BSA/Downloader.aspx?iDocumentStorageKey=238bc127-1b06-4272-a228-73747ae2d7f3&iFileTypeCode=PDF&iFileName=Cyber%20Security%20Considerations> (Accessed 29th July 2018)

## **Conclusion:**

After we introduced the numerous new threats and opportunities in the use and operations of cyberspace and understand the nature of cyber risk and distinguish cyber-risk for other kinds of risk as well as the adequate methods and techniques for cyber risk management. Here the proposed results and recommendations and have been made as a result of this work:

- 1) The Client or Insured should identify and evaluate the probability of several types of cyber risks
- 2) The difference between the cyber-attacks and risks including their financial impact
- 3) There are five inter-connected domains need to be used to guide in order to build a cyber-resilient organization capable of withstanding or recovering from cyber-attacks (Identify in order to develop an organization's understanding and management , Protect to covers all activities that will develop/update and implement effective precautions , Detect to identify any cyber security events, Respond to a detected cyber security event; Recover to how to plan a strategy to recover)
- 4) The Client have to choose the best option to deal with cyber risks: avoid, transfer, accept, or mitigate.
- 5) The Client has to setup their organization's risk management frame work and its process which must be decided as a part of the overall organization management as well as ensure that appropriate strategies are in place to provide a structure for managing and mitigating cyber risk
- 6) Clients should review their management of cyber risk to include mechanisms such as the establishment of a board risk committee and chief risk officer, the development of a joined-up recovery plan, and the use of stress-testing to confirm financial resilience against different high-risk scenarios including cyber
- 7) The Scope of cover under the cyber insurance product and how to tailor made the cyber all risks policy.
- 8) The Insurers or underwriters have to acquire the opportunity through arrange their risk assessment, policy wording, recruit the expert consultant and reinsurance program as well as taken the expertise of the global leader underwriters in the underwriting field.
- 9) The underwriters have to find solutions or innovation approaches to addressing the challenges to understanding cyber insurance coverage, supporting greater market capacity and managing of accumulation risks.
- 10) The underwriters have to learn how to manage the cyber insurance portfolio through enhance own cyber risk management capabilities to stay ahead of evolving threats, comply with new regulations and use its knowledge and insight for product development, deepen client engagement through joint development of cyber risk transfer products that fit the increasingly digital world and that differentiate themselves through ancillary services, collaborate with other insurers on market and cyber security firms for the benefit of all clients, develop cyber insurance products on a small scale
- 11) The underwriters have to monitor and pay attention for accumulated losses and business continuity plan
- 12) The underwriters have to enter into partnerships with information technology security firms to improve their access to information on incidents and accumulation.
- 13) The Regulator has to improve cyber security through regulation and collaborative efforts between government and the private sector to encourage voluntary improvements to enhance cyber security standards in order to eliminate such losses.
- 14) The Client and the underwriter have to identify the ranking of Cyber Risk Position of each industry



**Reference List:**

- 1) Allied Market Research, "Cyber Insurance Market to Reach \$14 Billion, Globally, by 2022".,Website Article Allison Berke,"15 Days of Cyber Insurance: Is cyber insurance health insurance?", Website article ,Stanford University
- 2) Aon Risk Solutions, Global Risk Management Survey 2017,Annual Report
- 3) appknox,"A Glance At The United States Cyber Security Laws", website Article
- 4) Becky Metivier,"How to Define Cyber security Risk", Website article
- 5) Becky Metivier,"Seven Characteristics of a Successful Information Security Policy", website article, Published on 8th February 2016
- 6) Becky Metivier;"6 Steps to a Cyber security Risk Assessment", website article, Published on 11st April 2017
- 7) Carter Schoenberg, "Cyber insurance in the 2018 regulatory landscape", Website Article , Published on 16th January 2018
- 8) Chartered Insurance Institute ,Insurance, legal and regulatory IF1 Study text: 2013-14
- 9) Chartered Insurance Institute, Reinsurance P97 Study text: 2015-16
- 10) Continuity central, "How to develop a Cyber Resilience Framework", Website Article, Published on 26th May 2017
- 11) Daniela GHETU,"PwC: Cyber insurance market set to reach USD 7.5 billion by 2020".,Websire Article ,Published on 28th September 2017
- 12) gc capital ideas; "Historical Development Of Cyber (Re)Insurance", Website Article , Published on 23rd October 2014
- 13) Green, Jeremy Swinfen,"Cyber Security: An Introduction for Non-Technical Managers",Routledge. 2015,eBook .
- 14) Green, Philip E. J.; Enterprise Risk Management: A Common Framework for the Entire Organization; Oxford: Butterworth-Heinemann. 2016;eBook
- 15) Hampton, John J.; "Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity"; Ed.: Second edition. New York: AMACOM. 2015;eBook
- 16) Heidi A. Strauß,"Cyber Risks(Threats – Trends – Mitigation)",Training presentation,2018 Münchener Rückversicherungs-Gesellschaft,Munich 2018
- 17) Hillson, David;"The Risk Management Handbook: A Practical Guide to Managing the Multiple Dimensions of Risk"; London: Kogan Page. 2016 ,EBook
- 18) Hiscox,"What is cyber and data risks insurance?", Cyber and data policy wording, Website Article
- 19) Institute of Risk Management , "Cyber risk", Website article
- 20) Insurance Journal, "Willis Towers Watson Adds Cyber Coverage to Aviation Offering", Website Article, Published on 28th February 2018
- 21) Jayleen R. Heft , "Top 10 writers of cyber security insurance", website article, published on 13th November 2017
- 22) John Munnings-Tomes &Jonathan Scott, "Cyber Security &Safety Considerations For Oil, Gas &Petrochemical Risk Assessment", Report belong to Lma Lloyd's
- 23) Juliann Walsh, "Protecting 'Flying Computers' "website article ,published on 5th July 2016

- 24) KELLY, BILL1,"4 Keys to Bridging the Cyber Insurance Gap." Article, Claims. Oct2017, Vol. 65 Issue 10
- 25) Kris Lahiri , "What Is General Data Protection Regulation? "Website Article Published on 14th February 2018
- 26) Le VPN,"ORIGIN OF CYBER SECURITY: WHEN DID INTERNET PRIVACY BECOME AN ISSUE? "Website Article , Published on 2nd October 2017
- 27) Lloyd's, "Cyber products at Lloyd's", website article
- 28) Lloyd's," Cyber Risk. Cyber Secure" ,YouTube video
- 29) Manners-Bell, John , "Supply Chain Risk : Understanding Emerging Threats to Global Supply Chains", EBook, London : Kogan Page. 2014
- 30) Marano, Pierpaolo-Rokas, Iōannēs- Kochenburger, Peter ; "The 'Dematerialized' Insurance : Distance Selling and Cyber Risks From an International Perspective", eBook., Switzerland : Springer. 2016
- 31) Martin Eling and JingjingZhu ; "Which Insurers Write Cyber Insurance? Evidence from the U.S. Property and Casualty Insurance Industry", e article, Journal of Insurance Issues, 2018, 41 (1)
- 32) MELISSA STEVENS,"4 Crucial Cyber Risk Management Steps Your Company Should Take Right Now", website article, Published on 31st May 2016
- 33) NATO Review, "The history of cyber-attacks", website article
- 34) OECD , "Enhancing the role of insurance in cyber risk management", Report, Date of publication 8 December 2017
- 35) Prowriters ; "The History of Cyber Insurance", Website Article, Published on 25th April 2016.
- 36) Queensland Government, "Cyber security insurance for Queensland Government agencies", Official Article ,last Reviewed 20th December 2017
- 37) Refsdal Atle-Solhaug Bjornar-Stølen Ketil,"Cyber-Risk Management", EBook, Springer 2015
- 38) Roger A. Grimes., "The 5 types of cyber-attack you're most likely to face", website article, Published on 21st August 2017
- 39) Taplin, Ruth, "Managing Cyber Risk in the Financial Sector: Lessons From Asia, Europe and the SA", E Book, London : Routledge. 2016
- 40) Ted Julian, "Defining Moments in the History of Cyber-Security and the Rise of Incident Response", website article ,Published on 4th December 2014
- 41) The European Centre of Technology, "THE IMPORTANCE OF CYBER SECURITY", Website article.
- 42) TOM BALL REPORTER, "Top 5 cyber insurance providers offering the best cover against attack", website article, published on 30th January 2018.
- 43) Ulsch, N. MacDonnell; "Cyber Threat! : How to Manage the Growing Risk of Cyber Attacks"; Wiley Corporate F & A Series; Hoboken, New Jersey : Wiley. 2014; EBook
- 44) Xprimm , "The EU cyber insurance market in the run-up to GDPR implementation", Website Article, Published on 26th April 2018.
- 45) Zainudin, Dyana1;Ur-Rahman, Atta1;"THE IMPACT OF THE LEADERSHIP ROLE ON HUMAN FAILURES IN THE FACE OF CYBER THREATS.", Journal of Information System Security. 2015, Vol. 11 Issue 2 ■

# 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

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.



**TRUST RE**  
REINSURER OF CHOICE

[WWW.TRUSTRE.COM](http://WWW.TRUSTRE.COM)