INSURANCE CONFERENCE 2022

STRENGTHENING RESILIENCE IN A CHANGING ECONOMIC LANDSCAPE – THE CASE OF INSURANCE

Topic: LOSS ADJUSTER DYNAMICS AND CHALLENGES IN SERVICE PROVISION

Speaker: STEVEN CHIZINGA

Organisation: INDEPENDENT ADJUSTERS LTD

IAZ INSURERS ASSOCIATION OF ZAMBIA

TAG Microinsurance Technical Advisory Group

IBAZ INSURANCE BROKERS ASSOCIATION OF ZAMBIA

PIA PENSIONS AND INSURANCE AUTHORITY

I have been asked to present a paper on the above subject.

I apologize if, to the more experienced, what I have to say may seem elementary. I am well aware that, to many, Loss Adjusting is not a familiar profession and is often misunderstood as a profession of experts whose role is to reduce amounts payable by Insurers.

LOSS ADJUSTER

Background

The Great Fire of London in 1666 heralded the beginnings of the loss adjusting profession, but it was not until 1941 that the term "Loss Adjuster" was used when the Association of Fire Adjusters was founded.

A number of prominent members of the profession formed themselves into a body called The Association of Fire Loss Adjusters. This was the first occasion on which the word Adjuster came into common usage.

A number of prominent members of the profession formed themselves into a body called The Association of Fire Loss Adjusters. This was the first occasion on which the word Adjuster came into common usage.

Earlier on to study for the Associate of the Chartered Institute of Loss Adjusters, the institute required the candidate to work in the UK, under a qualified Adjuster for a minimum period of 5 years as an Associate of the Chartered Insurance Institute or 3 years as a Fellow of the Chartered Insurance Institute, by examination.

Many changes have so far taken place and employees of an insurance organization can qualify to study for certificate courses and progress to the study of Associate of Chartered Institute of Loss Adjusters.

The Association began to exercise control over professional standards and conduct of their members.

In 1961, the Association was granted a Royal Charter and became The Chartered Institute of Loss Adjusters which received a Grant of Arm in 1979.

The Role of Loss Adjuster

"You say you are an Adjuster. What do you adjust? I only know my broker who has placed this insurance. "

The general public will be aware of the role of insurers or brokers, as when placing insurances, they will deal directly with insurer or broker.

In my opinion, a Loss Adjuster is an auditor of insurance claims. He is appointed by the insurer to handle claims on insurer's behalf and is expected by his principals to be within the confines of the policy. In otherwords, he has limited authority. He cannot vary the terms, conditions or warranties of the policy and should seek insurer's guidance on matters that are not clear from the policy documents. He should be familiar with insurance basic principles.

- Utmost Good faith
- Insurable Interest
- Contribution
- Subrogation
- Indemnity

- What is the subject matter of the policy? Or rather what property or liability is insured by the policy?

- What is the nature of the insurance or policy?

- What are the perils insured?

What are the policy:

i. Exclusions
ii. Conditions
iii. Warranties

- Who is insured under the policy?

The role of a Loss Adjuster is to apply the general principles of insurance to the loss. He will be guided by the policy, which is a contract of insurance that promises to pay within agreed terms, conditions, clauses and warranties. His duty therefore is to implement that promise by applying the basic insurance principles to claim settlement.

It is his duty to investigate the circumstances of the loss and to establish facts in order to ascertain whether policy liability exists and to what extent.

The first visit to the scene of loss is of particular importance. Evidence is fresh. Witnesses' memory is fresh. Damaged property may be undisturbed. Salvaging exercise can be implemented. Forensic investigations possible.

Will the loss lead to interruption to business, if so, does the company have a Business Interruption Policy? Agree with Insured measures to be taken in order to minimize business loss.

Report to Insurers on facts and opinions and make appropriate recommendations.

Always remember that the onus is on insured to prepare and present a claim in writing.

It is not the role of a Loss Adjuster to prepare a claim for Insured. Avoid litigation which may arise from your action. Insured may not agree with what you have stated in the claim and this could have serious legal implication.

Do not sign or endorse on any item on the claim form.

Your role is to check quantities and cost of damage or loss.

Property damaged must be the subject matter of the policy. Any item not falling within the definition of the policy must be excluded.

The peril causing the loss must be that named on the policy. If cover is All Risks, check for exclusions, such as ordinary wear and tear and depreciation.

Is the claimant named on the policy as Insured?

Is the loss address covered by the Policy?
Was the third party responsible for the loss? If so, start recovery exercise, with Insured's knowledge, with Insurer's knowledge.

Any salvage to be sold? Advertise for tenders, with consent of Insured, broker and insurer.

Use plain language as you discuss claim with policy holder. Avoid technical terms or explain and make the policyholder understand what you are talking about. No gamesmanship, that is, the art of winning without actually cheating. Stick to insurance principles.

CYBER CRIME CLAIMS

Can be complex.

Cyber criminal activity is conducted via internet.

The target of many attacks is a website and an organization's database.

This includes stealing an organization's intellectual property, confiscating online bank accounts, creating and distributing viruses on other computers, posting confidential business information on the internet.

A favorite target victim is the financial institution, which is a warehouse for money. A common scheme of the cyber criminal is falsifying debit/credit cards.

Attackers will steal debit/credit card data that can be skimmed on to a blank or discarded credit card and used to access the victim's credit or can be used online to buy articles for sale by the criminal

It is becoming increasingly essential for companies to effect a cyber insurance as the risk of cyber attacks against applications, devices, networks and users, grows. Loss or theft of data can significantly impact a business, from losing customers to the loss of reputation and revenue.

Preventive, detective and corrective controls implemented by an organization cannot completely eliminate cyber incidents and that may act as safe havens for the cyber criminals.

Cyber Insurance is a way to handle the residual risk. It is an insurance product used to protect organizations from internet based risk as well as that of other related IT activities, tools and processes. Hackers are becoming more forthcoming, using social media to disclose their exploits and compromised data. I can see a day when government and various industry regulators intensify pressure on businesses to protect personal data using significant fines for any breaches.

"Does your organization have an insurance policy that protects it from theft or misuse of electronic data or consumer records?

With the expansion of technology, especially the internet, organizations have reaped many benefits which come with some risks and threats, both to individuals and organizations. **One of these threats is cyber crime where bad guys do not wield guns and force to rob you, but use technology.**

Cyber criminals are capable of conducting sophiscated , crafty and creative attacks. **They target their victims and often these attacks are associated with cyber gangs that live in countries external to where the perpetrated organizations reside.**

Cyber insurance will include first party coverage, that is, losses that directly impact a company and third party coverage, which means losses suffered by other enterprises due to having a business relationship with the affected organization. The insurance will cover costs related to the remediation process, such as paying for the investigation, crisis communication, legal services and refunds to customers.

A cyber liability insurance policy will pay for recovery of data compromised by a cyber attack.

- The cost of repairing computer systems damaged by a cyber attack.

- Cyber attackers may demand fee from their victims to unlock or retrieve compromised data. Cyber insurance can cover costs of meeting extortion demands.

- Cyber insurance will cover costs incurred by a company for legal fees incurred through violating privacy policies or regulations or may hire computer forensic experts who will enable them to remediate the attack or recover compromised data.

The policy will exclude issues that were avoidable or caused by human error or negligence.

- Prior breaches, that is breaches prior to inception of policy
- Inside attacks – where an employee was responsible
- Pre-existing vulnerabilities
- Technology system improvements
- Ineffective security processes

It is difficult to investigate cyber crime because of anonymity that information and communication technology affords to users. Anonymity enables individuals to engage in activities without revealing themselves.

Cyber criminals can use anonymity networks to encrypt traffic and hide Internet Protocols Address in an effort to conceal their internet activities and location.

Anonymity networks mask users' identities and host their website via their hidden services capabilities which means that these sites can only be accessed by those on their anonymity networks.

Cyber criminals are often external to the victim.

The most costly attack is associated with malicious insiders, for example, an employee stealing funds via Electronic Funds Transfer or Wire Transfer.

Insurers should carry out a cyber audit of the proposer for cyber insurance coverage. The information obtained from the audit will enable the insurer to determine the type of insurance policy it can offer and at what premium.

It will take education and some diligence in developing controls and defences to thwart cyber crimes.

Firewalls, intrusion detection systems, vulnerability scanning and penetration testing, are primarily designed to protect the network from external threats.

A Loss Adjuster needs to investigate and understand how a cyber crime was perpetrated. He needs to investigate loopholes that allowed the breach to occur, how the cyber criminal got into the organization system, how to patch it and how to prevent it from happening again.

A Loss Adjuster needs to establish existing protections designed to protect the networks from external threats.

- Firewalls
- Intrusion detection system
- Vulnerability
- Penetration testing

A criminal organization called Lazarus launched malware on a bank's network for a while for purposes of stealing card data. This card data was then sold on the black market called the black hole.

The first area of attack was personal emails before targeting the servers that hold account holders information. Card theft went on for a while but, when changes to the bank's risk profile was enacted, this allowed the hackers to access the accounts and transfer funds to private accounts domiciled in Brazil.

SIM SWAP CLAIMS

I happened to deal with a Sim Swap loss and will share my observations with you.

The fraudsters replaced existing customers' SIM Cards which were linked to Bank Accounts with NEW SIM CARDS which they had acquired and connected their acquired SIM cards to existing customers phone numbers which were linked to customers' accounts. Thereafter, the skimmers phoned the customer call centre at the bank using customers' phone number asking for Pin/Password reset for Mobile Banking and Internet banking.

Having succeeded in getting Pin/Password reset, they became owners of the accounts and performed several spurious transactions on the accounts through Mobile Internet Banking, involving a substantial sum of money which was transferred to accounts opened at the bank for the purposes of receiving stolen money.

Insured were unable to provide particulars of SIM CARDS which fraudsters had acquired from mobile service providers, for the purpose of perpetrating the fraud. They argued that this is a matter for mobile service providers over whom they have no control.

The SIM CARDS might have provided:

- Full identity of the fraudsters
- Details of the mobile service provider who no doubt will have to demonstrate that they had complied with legal requirements with regard to issuance of sim cards.

The mobile numbers used to steal money from bank customers' accounts are known and documents in this regard should be available.

Fraudsters can take over customers' accounts by tricking them into handing over personal information which can be used to access customers' bank accounts or even take over mobile services to intercept security codes and alert messages.

Sim swap fraud exploits a mobile phone service provider's ability to seamlessly port a phone number to a device containing a different Subscriber Identity Module (SIM). This feature is normally used when a customer has lost or had his phone stolen, or is switching service to a new phone.

The scam begins with a fraudster gathering personal details about the victim, either by use of phishing emails or by buying them from organized criminals.

Once the fraudster has obtained these details, he then contacts the victim's mobile telephone provider. The fraudster uses social engineering techniques to convince the telephone company to port the victim's phone number to the fraudster's SIM. This is done, for example, by impersonating the victim using personal details to appear authentic and claiming that they have lost their phone.

In many cases, SIM numbers are changed directly by telecom company employees bribed by criminals.

Once this happens, the victim's phone will lose connection to the network, and the fraudster will receive all the SMS and voice calls intended for the victim. This allows the fraudster to intercept any one-time passwords sent via text or telephone calls sent to the victim and thus allows them to circumvent authentication methods of accounts that rely on text messages or telephone calls.

Do not share details of:

- Bank statements
- Passport
- Driver's licence

Keep digital copies of these documents securely.

Do not respond to unsolicited emails that ask for personal information.

It might be difficult to establish that the employee acted to benefit from the fraud or was negligent in disclosing customer's banking information.

There is need for Mobile Network Operators and Financial Institutions to share client information, notwithstanding data protection regulations. This will go a long way in controlling cyber crime.

IN MY OPINION, A STAND ALONE POLICY COVERING CYBER RISKS SHOULD BE CONSIDERED.

COVID 19 – B.I. CLAIMS

Adjustment of Business Interruption loss following outbreak can present problems.

On 13th March 2020, the first death of a person who had been tested positive for COVID 19 was recorded in Zambia.

In January 2020, the World Health Organisation announced that a coronavirus had been traced in samples obtained from the cases in China. The virus was named SEVERE ACUTE RESPIRATORY SYNDROME CORONAVIRUS 2 (SARS – COV 2) and the associated disease was named “COVID – 19”.

World Health Organisation declared the outbreak of COVID-19 a “PUBLIC HEALTH EMERGENCY OF INTERNATIONAL CONCERN,” on 30th January, 2020.

ON 11th March 2020, the World Health Organisation declared COVID -19, to be a pandemic.

On 13th March 2020, the Minister of Health issued STATUTORY INSTRUMENT No. 22 which makes COVID 19 a notifiable disease in Zambia.

Night clubs, theatres, cinemas, gyms, leisure centres were forced to close down. Restaurants, cafes, bars and public houses, were required to close or cease carrying on the business of selling food and drink other than for consumption off the premises.

Some companies had a skeleton staff at the offices, whilst other workers were operating from home.

THE STANDARD BUSINESS INTERRUPTION POLICY

This follows closely the style of the standard fire policy. It specifies that;

- The premium having been paid
- "Damage" having occurred
- Interruption to the business having resulted from such damage
- Loss having resulted from such interruption

Then the company will pay to the Insured the amount of loss ascertained in accordance with the provisions of the policy. **There must be damage, causing interruption, resulting in loss.** The chain of causation must be unbroken.

So, the basic cover provided by this section is for Business Interruption which is a consequence of physical loss or destruction of or damage to property insured under the property damage section of the policy.

The key requirements for a claim under the Business Interruption Policy are that there must be damage **to property owned or used by the insured at the premises for the purpose of the business. The property should be the subject matter of the policy**

Insured Event

"Interruption of or interference with the Business in consequence of damage referred to in the corresponding Material Damage insurance which shall mean the property damage… **covering the interest of the insured but only in respect of perils insured and property not specifically excluded under the property damage …**

The B.I loss must flow from interruption or interference with insured's business.
However, the policy contains a series of extensions which provide for Business Interruption that is not consequent on physical damage to property.

The critical extensions for present purposes are

A. INFECTIOUS DISEASE AND NOTIFIABLE DISEASES"
B. DENIAL OF ACCESS

The definition of Damage shall be deemed to include interruption of or interference with the Business as defined caused by the following contingencies:

1.1 Notifiable diseases

<u>An outbreak of which the competent local authority has stipulated shall be notified to them.</u>

For the purpose of this extension, an area within a stipulated radius from the Insured premises is included.

Notifiable disease is a contingency and the policy covers Business Interruption losses resulting from the occurrence of a notifiable disease such as COVID 19 at or within a stipulated radius from the Insured premises. Notifiable disease should be regarded as a peril insured. In other words COVID 19 is an insured peril.

B. DENIAL OF ACCESS

This is a specific extension which states " This insurance extends to include loss resulting from interruption of or interference with the Business in consequence of Damage to any property by an Insured peril in the vicinity of the Insured's premises which shall wholly or partially block or prevent access thereto provided that for the purpose of this Specific Extension "in the vicinity" is deemed to mean within a radius of 10km of the perimeter of the Insured's premises.

Clearly, the Extension provides cover for business Interruption losses resulting from public authority intervention preventing or hindering access to or use of the business premises.

The B.I Loss must flow from interruption or interference with the business of insured.

IN OTHERWORDS, JUST BECAUSE THERE HAS BEEN AN OUTBREAK WITHIN THE SPECIFIED DISTANCE OF 10KM IN THE POLICY DOES NOT MEAN THAT THE POLICY HOLDER'S BUSINESS INTERRUPTION LOSS FLOWS FROM THAT. ACT OF AUTHORITY REQUIRES PREVENTION OR DENIAL OF ACCESSS TO BUSINESSES.

THE DENIAL OF ACCESS CLAUSE CAN APPLY ONLY WHERE THERE ARE RESTRICTIONS IMPOSED BY A PUBLIC AUTHORITY, FOLLOWING AN OCCURRENCE OF A NOTIFIABLE DISEASE. AN INSTRUCTION GIVEN BY A PUBLIC AUTHORITY MAY AMOUNT TO A RESTRICTION IMPOSED IF IT CARRIES THE IMMINENT THREAT OF LEGAL COMPULSION. THE BUSINESS INTERRUPTION LOSS SHOULD RESULT FROM INSURED'S INABILITY TO USE THE INSURED PREMISES, COMPLETELY NOT PARTIALLY.

A standard Business Interruption Policy may provide cover as follows:
Cover for other events is as follows:

“Loss following interruption of or interference with the business in consequence of murder, rape, suicide, food or drink poisoning, contagious or infectious diseases, vermin, pests, or defective sanitary arrangements occurring at the premises or wild animal attack within 5 km (five kilometres) or bomb threat or oil spill within 15 km (fifteen kilometres) of the premises to which this insurance relates.”

Murder, rape, suicide, food or drink poisoning at Insured premises.

Cover in this case applies to interruption to business resulting from non operation of Insured's business due to murder, rape, suicide, food or drink poisoning of Insured and or employees.

Contagious and Infectious Diseases

There is cover for interruption to business resulting from Insured or indeed Insured's employees being unable to carry on the business because they have been attacked by infectious diseases.

If Insured can show that they were unable to carry on the business at **Insured premises** because their employees **at the premises** had been attacked by say a contagious disease and that the premises were thus closed for business, they would merit a claim.

A medical report will be required in support of the claim.

Let it be said that, it should not be customers who should be victims of murder, rape, suicide, food or drink poisoning for Insured to sustain a claim under this extension.

Cover is for Insured or their employees who might have been victims of murder, rape, suicide, food or drink poisoning, contagious disease **at Insured premises.**

LOSS ADJUSTER – FUTURE

The challenge for Loss Adjusters is to provide a responsive and dynamic service to the market with well placed specialist adjusters to respond to more complex losses such as Business Interruption and subsidence claims.

There is a vibrant future for specialist adjusters.

- Brokers and general public likely to involve experienced adjusters to handle complex claims on behalf of their clients.

- Climate change, technological advancements, viruses likely to create large and complex losses which will require the involvement of specialist adjusters. Insurers will not have staff capable of handling complex claims.

- The breadth of work undertaken by adjusters will be much wider involving a range of skills.

- Loss adjusting companies are likely to suffer from intense competition brought about by insurers superimposing low fee scales and demanding retroactive quantity discounts, against a background of many insurers seeking to carry out more work in-house.

THANK YOU!!!