International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 01-02-2025, Accepted: 03-03-2025, Published: 19-03-2025
Volume 7, Issue 1, 2025, Page No. 92-98

Protecting E-commerce stakeholders through the insurance and cryptographic mechanisms: A legal perspective

Mc Levis Lynne Junior
Department of English Law, Faculty of Law and Political Science, University of Dschang, Cameroon

Abstract
The manifestations of electronic contracts are sometimes plagued with hurdles tending to make fulfillment/enforcement of such contracts difficult. These hurdles stem from the overall nature of the transaction, as it is concluded in a sphere where parties are not in physical contact or are unable to transact face-to-face. This therefore causes some complexities to contracting parties as to whether bargains, responsibilities and security engagements under the contract shall be met. A lean towards protection of stakeholders' interests and more particularly of rights and obligations under the contract against breaches/violations is therefore worthwhile. In this regard, the insurance and cryptographic mechanisms can be considered as some measures intended for the protection of stakeholders/parties in electronic commerce contracts. Therefore, this write-up holds that, stakeholders in electronic commerce also require protection by way of insurance and the crypto system in order to ensure that the stakes of the contract are fulfilled, and also that breaches are averted. As such, the objective of this research is to ascertain how insurance and the crypto system can be used as veritable mechanisms to ensure a fulfilling contract between contracting parties to an electronic commerce transaction.

Keywords: Protection, E-commerce, stakeholders, insurance, cryptography, mechanism

Introduction

A typical facet of electronic contracts has to do with the tendency to protect the stakes of the contract. This is paramount as the need to realize a fulfilling electronic commerce transaction becomes desirable and worthwhile. The necessity to protect stakeholders/parties in electronic commerce is therefore indispensable, as it proves to be a fundamental factor determining the success of the electronic contract. Mindful of the fact that electronic commerce transactions most often poses threats of insecurity to the parties involved, there becomes the need for parties to ensure that their transaction is within safe margins and capable of being realized. This is especially due to the fact that the use of such ubiquitous technology is not assuming apex of its success owing to the menace of security issues that have become a matter of great concern to the customers as well as to the online provider [1].

In the cyberspace for example, both the client and the vendor experience issues in demonstrating their personality to one another with certainty, especially during a first transaction [2]. This creates some complexity in reaching a favourable contract outcome. This becomes even more pressing with the presence of consumers in the transaction who are considered to be more susceptible to commercial malpractices in the electronic commerce arrangement, such as deceit/fraud, infringement on privacy and/or intellectual property rights, non-performance of contractual obligation(s) and a host of others. This is why it is said that transactions such as the sale of goods via the Internet are vulnerable to violations of consumer rights since there is no meeting between the consumers and businesses at the time of the transaction [3]. The parties/stakeholders in electronic commerce transactions therefore need a framework for the protection of their rights under the contract, which shall go a long way to provide the parties with the guarantee or assurance they need for the contract to be executed and accomplished pacifically and within the stipulated time frame. This can be achieved through the insurance and cryptographic mechanisms as discussed below.

The Insurance Mechanism of Protecting Stakeholders in Electronic Commerce Transactions

Stakeholders [4]/parties in electronic commerce transactions can protect their rights and ensure performance of obligations under the electronic contract through insurance coverage or policy schemes. This is why electronic trading or e-commerce transaction is an object of insurance, because all activities in electronic transactions or e-commerce can cause loss, damage or not get the expected profit for the parties involved [5]. Aware of the fact that there could be risk, loss or damage of executing certain activities and/or obligations under the electronic sales/commercial transaction; such as those pertaining to delivery, conformity and safeness of a product/good, and also those relating to privacy engagement of services through online platforms, the requirement of insurance coverage is therefore worthwhile in these cases.

Moreover, it is the researcher's view that since buyers in electronic commerce are not accustomed to the practices and operations of most commercial transactions performed electronically by sellers through their platforms, it is only fair and normal that, sellers/producers/suppliers undertake insurance schemes in relation to their transactions or activities (which mostly comprise of selling their products) with buyers or the public at large as way of securing the transaction and boosting customer trust and confidence. And this requirement of insurance particularly behooves them if it is requested by buyers in order to secure their rights under the contract. The justification for this is that, sellers are generally versed in the business they do, and as such know the risks and implications involved in their commercial dealings with the public. The insurance policies in this context is most often taken in favour of the buyer/purchaser (considered in the insurance contract as a third party) who

stands at a losing side if the good(s) ordered do not finally reach him, or are found to be defective or unsuitable for the intended purpose. It serves as some form of compensation/indemnity for non-execution, wrong/improper delivery, damage/injury, and a host of others.

Insurance can therefore be defined as a contract whereby a person called the insurer or assurer, agrees in consideration of money paid to him, called the premium, by another person, called the insured or assured, to indemnity the latter against loss resulting to him on the happening of certain events [6]. This is why it was stated by Channell J in *Prudential Insurance Co v IRC* [7], that there are three requirements for a valid contract of insurance. First, it should provide some benefit for the policy holder on occurrence of some event, secondly, the occurrence should involve some element of uncertainty; and thirdly the uncertain event should be one which is *prima facie* adverse to the interest of the assured. The judge then added that this was not an exhaustive definition [8]. Harvy Ivamy also goes further to define insurance as a contract whereby a person called the "insurer" undertakes, in return for the agreed consideration called the "premium", to pay to another person called the "assured", a sum of money or its equivalent on the happening of a specific event [9]. A look at these definitions indicates that a typical insurance contract involves two parties, that is the insurer and the insured/assured. And it also involves premiums furnished in order to indemnify the policy holder or any named person in the contract in the event of a certain occurrence for which the policy was undertaken.

Within the electronic commerce environment, insurance schemes can be looked at as one of those essential ways or mechanisms to guarantee or protect the interest and entitlements of parties/stakeholders in electronic commerce contracts. For example, marine insurance can be taken to guarantee the safe delivery of goods in the course of the voyage, or to ensure that the goods reach the buyer safely and in good condition. Similarly, product liability insurance can also be taken by sellers to guard against any defect or damage that their products may cause to the buyer. The insurance business in electronic commerce is therefore not to be overlooked as far as the e-commerce contract is a going concern.

The Fundamental Purpose of Insurance Contracts

It follows that the fundamental purpose of insurance is to provide a means for upsetting the burden of physical, financial, psychological and/or virtual loss/damage. In other words, it is to compensate or indemnify the victim for damage, losses or injuries incurred as a result of an unforeseen circumstance. Insurance neither eliminates the loss, nor does it undertake to stop the misfortune or disaster from happening [10]. All it does is to help soften the blow from a purely economic view point [11]. It therefore provides a safety net for unforeseen events. This is why it is sometimes considered to be a financial protection or mitigation tool against possible unforeseen hardships. The insurer assesses the possible hardship and pays in line with the agreed policy. Such an amount is termed "Sum Assured" or "Sum Insured" or "Insured Value" etc. this gives essence to the insurance policy and increases the desire of policy seekers.

Categories of E-Commerce Insurance Schemes

At this level, it is of interest to consider some insurance policy schemes that can possibly operate within the e-commerce environment, and especially for the purpose of protecting parties in such arrangement. It is also worth noting that, consideration of these schemes here is not exhaustive, as it could behoove parties to take up other insurance policies depending on the stakes of their transaction.

Liability Insurance

Aware of the fact that business enterprises, professionals and individuals are exposed to various types of risks, of which liability risks are important with probable far-reaching detrimental financial consequences [12], there is the tendency for stakeholders in commercial transactions, most especially businesses/companies to start looking for ways to surmount the burden of loss or damage caused by their activities. Liability insurance therefore comes into play, and it acts as a fundamental insurance scheme that covers or is part of the general system of risk transference, designed to offer specific protection against third party claims, i.e., payment is not typically made to the insured, but rather to someone suffering loss who is not a party to the insurance contract.

This type of insurance (also known as third-party insurance) is a part of the general insurance system of risk financing to protect the insured (the purchaser of the insurance policy) from the risk of liabilities imposed by lawsuits and similar claims and protects the insured if the purchaser is sued for claims that come within the coverage of the insurance policy [13]. It provides protection against claims resulting from injuries and damage to people/or property. It also covers legal costs and payouts for which the insured party would be found liable, with exclusion to intentional damage, contractual liabilities, and criminal prosecution. This category of insurance is suitable for commercial transactions undertaken by businesses, companies and even private individuals who on daily basis operate with the public, in terms of the purchase, procurement, consumption and/or delivery of their products or services to customers. This insurance scheme is made up of product liability insurance and professional liability insurance as seen below.

Product Liability Insurance

This is an essential component of liability insurance, and it relates specifically to products or goods that sellers/suppliers/producers make available to the public for purchase/consumption. This insurance scheme protects against the cost of compensation for personal injuries caused by faulty products, loss of or damage to property caused by such products and even unforeseeable circumstances such as product faults that quality control systems could not identify. Most businesses will have to consider this insurance scheme as a veritable mechanism to cover any injuries or damage caused by the use or consumption of their products by third parties. The indemnities under this head are therefore in the interest of third parties (consumers/customers) who get affected by the product sold to them by businesses. It is therefore the researcher's view that such an insurance scheme should be observed or even considered by e-commerce businesses/platforms while carrying out their activities of selling and marketing, since the products or services they

offer cannot be hundred percent assured of their satisfactory quality and safeness, in a bid to avert harm, damage or loss to the buyer/purchaser.

Professional Liability Insurance

This is a form of liability insurance that provides coverage for professionals and businesses to protect against claims of negligence, errors or omissions from clients or customers in the exercise of their activity. It typically covers negligence, IP infringement, personal injury, and more. The coverage essentially focuses on alleged failure to perform on the part of, financial loss caused by, and error or omissions in the service or product sold by the policyholder. These are causes for legal action that would not be covered by a more general liability insurance policy which addresses more direct forms of harm. The primary reason for professional liability coverage is that a typical general liability insurance policy will respond only to a bodily injury, property damage, personal injury or advertising injury claim.

However, various professional services and products can give rise to legal claims without causing any of the specific types of harm covered by such policies. Common claims that professional liability insurance covers are negligence, misrepresentation, violation of good faith, and inaccurate advice. For example, if a certain good (let's say a car) was ordered and purchased electronically, but upon delivery, it was found to be a motorcycle, contrary to what was ordered by the buyer based on the business advert. This may amount to misrepresentation and the purchaser can institute an action for redress. When this happens, businesses that have a liability insurance cover can be less burdened by this situation, as their insurance will indemnify the third party (purchaser of the good).

Professional liability insurance policies are generally set up based on a claims-made and reported basis, meaning that the policy covers only those claims made and reported to their carrier during the policy period [14]. More specifically, a typical policy will provide indemnity to the insured against loss arising from any claim or claims made during the policy period by reason of any covered error, omission or negligent act committed in the conduct of the insured's professional business during the policy period. This insurance scheme is also instrumental in electronic commerce transactions, as it covers against any fault committed by the dealer, vendor, producer or supplier in the course of business.

Cyber Insurance

Another pertinent insurance scheme necessary for the protection of stakeholders in electronic commerce is 'cyber insurance' (also known as cyber-security insurance). Although insurance companies have been insuring all kinds of products and catastrophic events for hundreds of years, cyber insurance, which covers a company's losses and costs stemming from a cyber-attack, is a relatively new concept [15]. This type of insurance is worthwhile especially based on the recurrent and prevalent nature of cyber risk which remains among the top risks facing business organizations today [16]. Cyber-security insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption and network damage. A robust cyber-security insurance market could help reduce the number of successful cyber-attacks by; promoting the adoption of preventive measures in return for more coverage, and encouraging the implementation of best practices by basing premiums on an insured's level of self-protection [17].

Cyber insurance allows companies to transfer some of the financial risk associated with cyber incidents to an insurer. It is intended to cover business liability, including first-party costs, and is often presented as a critical component of cyber risk-management approaches within organizations [18]. It equally follows that the increased reliance on digital technologies has led increasing digital security and privacy risks and the emergence of a cyber-insurance market to provide policyholders with financial protection against many of those risks [19]. The affirmative cyber insurance market (i.e., stand-alone cyber insurance policies and cyber endorsements added to other policies) is focused on protecting businesses against some of the consequences of six main types of (mostly malicious) cyber incidents [20]:

- Data confidentiality breaches (including privacy breaches): where a company has allowed (or has not prevented) unauthorized access to the private information (financial, medical, biometric, commercial) of individuals or companies resulting in incident management and notification costs, data, software and hardware restoration costs, legal and defense costs, compensation to injured parties and fines and penalties (regulatory and/or contractual.
- Network security liability, as in where a company has allowed (or has not prevented) the use of its network in a cyber-attack on a third party leading to legal and defense costs and compensation to injured parties.
- Communication and media liability: where a company's digital communications activities (intentional or accidental) result in defamation, libel, slander or other harm to a third party leading to legal and defense costs and compensation to injured parties.
- Technology disruptions: where a company's operations have been disrupted as a result of a technology failure (accidental or malicious) at the company or one of its service providers leading to business interruption losses (or contingent business interruption losses) and potentially data, software and hardware restoration costs.
- Cyber extortion: where a company's ability to access its data (or network) has been compromised or breached as part of an extortion (ransomware) attempt, leading to incident management costs, financial losses (ransom payment) and/or business interruption and data, software and hardware restoration costs; and
- Cyber fraud and theft: where a company's funds or assets are stolen or fraudulently expropriated, including through social engineering, resulting in financial losses [21].

In effect, this insurance scheme is meant to provide coverage options and pre-conditions that need to be considered when purchasing the policy; such as, first party coverage that protects against losses incurred directly by the company in response to a cyber-incident (direct expense), and typically includes theft and fraud, forensic investigations, business interruption, extortion, and computer data loss and restoration. And secondly, it also provides third party coverage that protects against losses incurred by third parties in response to a cyber-incident, and typically includes litigation, dealings with regulators, notification costs, crisis management and credit monitoring [22].

Marine Cargo Insurance

This is yet another important insurance coverage mechanism in commercial transactions, and precisely in protecting the interest of the buyer-purchaser who expects his good/product to be delivered/ transported as per stipulations in the contract of sale. Marine insurance generally covers any peril during transportation by sea from one destination to another [23]. This is mostly witnessed in international sale transactions or cross border commerce, where one enters into a contract of sale with another (generally the contracting parties resident in different countries) for the purchase and supply/delivery of a particular good/product. And it is then agreed in the contract that such good will be transported/shipped from the seller's place of business to the buyer's location. In this situation, in order to guard against risk or sea peril, a marine cargo insurance policy is therefore undertaken for the purpose of the voyage, and particularly to protect the interest of the buyer in the good in case there is an unforeseen occurrence at sea causing damage to cargo or the entire vessel [24]. This is why international trade is often considered as a risky venture as any business deal. And though there is no law to make the insurance of property in transit a mandatory precaution, risks of commerce can be minimized by being properly insured [25].

With this kind of insurance scheme, several forms of claims can occur, including total loss and partial loss [26]. Even though it only uses one ship that sails from one port to another, several cargoes are belongings to more than one shipper. Each of these marine cargoes must be insured, which means that several important insurance policies must be used even for one vessel and one voyage [27]. It is equally noteworthy that a contract of marine insurance is one in which the utmost good faith must be observed. Every material circumstance which is known to the insured must be disclosed to the insurer. A circumstance is material if it will influence the judgment of the insurer in fixing the premium or accepting the risk. Hence in the English case of *Russel v Thornton* [28], the concealment of the fact that the ship had grounded and leaking before the insurance was effected, was held to be material to the contract.

Ship cargo claim procedure

When damage occurs to goods, the actions to be taken by the insured comprises of stating an occurrence of a loss or damage, request a survey (contract an insurer correspondent), and to mitigate damage [29]. In the eventuality that goods are destroyed, damaged, or stolen, a marine insurance claim in writing should be made to the insurance company immediately so that they can take the necessary steps to determine the loss. Claims may be submitted either by the legal owner of the damaged freight, or an entity accepting risk of loss in transit, or a legal proxy. The claim must be made to the carrier or the shipping company. A formal acknowledgment also needs to be received from both the insurer and the shipping company. It may be necessary to make a claim to all the carriers in the transit chain.

In addition, there may be occasions where third parties other than the carriers (stevedores, port authorities, custom authorities, etc.) may be liable for loss or damage. All documentation pertaining to claims against such third parties must be preserved. Failure to comply with this requirement will prejudice insurance claims. Finally, for underwriters to be able to conclude the claim with the carrier or third party, after having paid for the claim to the insured under subrogation, the former must be held responsible, in writing, by the claimant, for the loss within a specific time frame [30]. In summary, the procedure involves [31];

- Immediately notifying the insurer or underwriter, or contact the shipping line customer service
- Appoint a surveyor and arrange for joint/bilateral inspections of the damage cargo
- Minimize and prevent further losses
- Collect documents regarding the claim
- Submit a substantiated and quantified claim
- Protect against time bar [32].

Furthermore, certain documents relevant to the claim may also be required from the insured; such an original insurance policy or certificate, bill of lading (or other carrier's receipt), survey report, original invoice and packaging list together with shipping specification, weight notes, bill of sale, sea protest and letter of subrogation [33]. These documents are therefore important in determining the nature and extent of the damage or loss requiring indemnity.

The Working Mechanism of Cryptography in Protecting Stakeholders in Electronic Commerce Transactions

This is another vital mechanism in protecting the rights and obligations of stakeholders/parties in electronic commerce transactions. Particular concerns here are in response to data protection and/or information security within the electronic commerce environment. Since security attacks are being associated in e-commerce, the use of cryptography provides highly secure and efficient framework for e-commerce transactions, so that it uses different encryption and decryption techniques [34]. Moreover, as the importance of information systems for society and the global economy intensifies, systems and data are increasingly exposed to a variety of threats, such as unauthorized access and use, misappropriation, alteration and destruction [35]. The word cryptography comes from the Greek word *Kruptós logos* meaning *hidden word* and has been used for "secret writing" for many years [36]. It is also considered by this Greek appellation as the science and art of code-making and code-breaking. Cryptography in more elaborate and simpler terms is the art of "creating and using methods of distinguishing messages, using codes, ciphers, and other methods" so that only the intended person can receive the information [37]. It has also been defined by the Cameroon Cyber Law as "the use of mathematical algorithm to encrypt information in an attempt to make it unintelligible to those who are not authorized to access it" [38].

Cryptography makes sure that secrecy is maintained between the sender and the receiver. With the advent of new technology and a greater need to protect them, the use of cryptography has increased exponentially [39]. This goes a long way to protect the security of information, customer data, product data, and protection from theft, which of course is done through the use of built-in encryption techniques that provide high data security [40]. It is in this light that, the use of the cryptographic technique is therefore instrumental in safeguarding the rights and interests of parties in electronic commerce transactions, especially those pertaining to privacy and data/information security.

Cryptographic Techniques

Several cryptographic techniques can be employed in order to ensure its proper identification, functioning and application in electronic transactions, and especially since it has as main goal to secure information and ensure efficient usage and manipulation [41]. These techniques as seen below are considered to be essential in determining how cryptography works.

a. Conventional or Symmetric Cryptography

Symmetric cryptography is the most traditional form of cryptography. In a symmetric cryptosystem, the involved parties share a common secret (password, pass phrase, or key). Data is encrypted and decrypted using the same key [42]. These algorithms tend to be comparatively fast, but they cannot be used unless the involved parties have already exchanged keys [43]. The sender uses a key to encrypt the message and the receiver uses the same key to decrypt the message. For this to happen, the sender and the receiver must generate, share, and store the key in advance. However, this technique has a couple of difficulties or inadequacies. First, since most transactions over the internet occur between parties that do not have an established prior relationship, they cannot share the key in advance, second, exchange of keys will lead to deferments of transactions; third, each person will have to retain a different key for each person he or she wishes to communicate or transact with; and forth, it will become difficult for the parties to securely exchange the keys. This key management problem was effectively solved by asymmetric or public key cryptography [44]. Examples of this crypto method include; Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES, and Blowfish.

b. Asymmetric cryptography (public/private key Cryptography)

This is a technique which consist of different keys used for both encryption and decryption process. One key is called public key and another is called private key. The public key is used for encrypting the original message, whereas the private key is used to decrypt the message. Both public and private key are generated by the receiver. Later, the receiver distributes the public key to the sender through a public-key distribution channel. Asymmetric key cryptography can be used for authentication, digital signatures and secret key exchanges [45]. It has advantages in that, only the private key must be kept secret. Depending on the mode of usage, private key/public key pair may remain unchanged for considerable periods of time, which makes this cryptographic technique more reliable. Also, many public-key schemes yield relatively efficient digital signature mechanisms, and in a large network, the number of keys necessarily may be smaller than in the symmetric-key scenario [46]. This technique is very useful especially when it concerns online activities that call into play a substantial number of persons transacting through the medium of the internet. It helps to assure security of information and correspondence through the use of the public/private keys, which cannot be accessed easily by just any individual without having to go through a verified authentication process. This is particularly the case with organizations/ businesses that operate electronically with different customers who are expected to verify/authenticate their identity/details through the asymmetric crypto system before proceeding with the transaction. However, this technique's ability to initiate a secure communication channel between two parties who have never communicated before has made the growth of e-commerce possible on the internet [47]. Examples of this type of crypto technique includes; RSA, Elliptic Curve Cryptography (ECC), Diffie-Hellman (DH).

c. Visual Cryptography

This is another crypto technique used in achieving data security in electronic transactions. Visual cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is possible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information [48]. This method has proven to be a secure and reliable cryptographic method and hence application of this method has increased. It has proven useful in watermarking, anti-phishing systems, human machine identification, secure banking communication, and offline QR Code authorization [49]. It is even used in many real-time applications such as transmitting passwords, authentication, and information forensics and more. This technique is also worth considering in securing data/information passed through the internet, and especially in electronic transactions.

Stakeholders in electronic commerce must equally look into this aspect of cryptography, as another mechanism to secure/protect their rights (especially that of privacy) which most often comprises of sensitive information, details or correspondence circulated between the parties on the internet. This mechanism also fights against cybercrimes.

Conclusion

Looking at the nature of commercial transactions concluded online, individuals, organizations and businesses must all be wary of their dealings via this medium of transacting. And with the current prevalence and trends of cyber-attacks and fraudulent/dubious practices perpetrated by internet users, there is the tendency to ensure some degree of security or protection of stakeholders' interests in electronic commerce transactions. The Insurance and cryptographic schemes are therefore mechanisms to ensure the protection of stakeholders in electronic commerce, especially that of ensuring that rights and obligations under the electronic contract are executed with caution, failure of which will give rise to damages in the event of breaches.

Reference

1. Nuwan k *et al*., A Systematic Review of Security in Electronic Commerce: Threats and Frameworks, Global Journal of Computer Science and Technology,2019:19(1):33.
2. Ajam NH. Enhanced the Security of Electronic Commerce, *Journal of Babylon University/Pure and Applied Science*,2016:24:1174.
3. Fibrianti Nurul Consumer Protection in Electronic Transactions, *International Journal of Business, Economics and Law*,2017:12(4):64.
4. This will include the buyer and seller as principal stakeholders, and intermediaries, E-commerce

platforms/companies, internet service providers etc., as secondary stakeholders. A stakeholder is generally considered to be anyone who is involved in or affected by a course of action (which for the purpose of this write-up could be the direct parties to the electronic contract (buyer and seller), and/or third parties). It could equally denote an individual, group or organization that is impacted by the outcome of a project or a business venture. Although the term stakeholder is rarely used in the electronic commerce literature there is extensive reference to the "players" [IMRG, Electronic Commerce in Europe. *An action plan for the marketplace*.1998, IMRG (Interactive Media in Retail Group) taking part in the electronic commerce marketplace. The terms that are usually used and refer to particular sets of interests are: global customers, trading partners, electronic commerce experts, information technology vendors, internet providers, competitors, government, trusted third parties etc (Anastasia p et.,al), Applying the stakeholder concept to electronic commerce: extending previous research to guide government policy makers, *Proceedings of the 34th Hawaii International Conference on System Sciences, 2001*.

5. Riyanto Mochamad S. H, Electronic Transaction on Insurance in Legal Perspective, *International Journal of Business, Economics and Law*,2018:16(5):272.
6. Simon TT. Lecture Notes on Insurance Law, University of Dschang, unpublished, 2021, 6. [1904] 2 KB 658.
7. Hodgin Ray, *Insurance Law, Text and Materials*, 2nd edition, Cavendish Publishing Limited, 2002.
8. The Glass House, Wharton Street, London, United Kingdom, p 1.
9. Simon T.T, *op. cit*, p 6.
10. *Ibid*.
11. *Ibid*.
12. Anderson SE, *et al*., The Underwriting Process of Liability Insurance in South Africa, *Risk Governance Control: Financial Markets and Institutions*,2014:4(1):46.
13. Originally, individual companies that faced a common peril formed a group and created a self-help fund out of which to pay compensation should any member incur loss (in other words, a mutual insurance arrangement). The modern system relies on dedicated carriers, usually for profit, to offer protection against specific perils in consideration of a premium.
14. Mendoza MA. The Limits of Insurance As Governance: Professional Liability Coverage for Civil Rights Claims Against Public School Districts, *Quinnipiac Law Review*,2020:38:379.
15. Nieves A, Cyber Insurance Today: Saving It Before It Needs Saving, *Catholic University Journal of Law and Technology*,2020:29(1):112.
16. Strupczewski G, The Concept of Cyber Insurance and Its Role in the ISO-Risk Management Process: An Industrial Perspective, *Cyber security and Law*,2023:10(2):364.
17. *Ibid*, p 13.
18. Sullivan J, Nurse JR. Cyber Security Incentives and the Role of Cyber Insurance, *Royal United Service Institute for Defense and Security Studies*, 2020, 4.
19. OECD, The Role of Public Policy and Regulation in Encouraging Clarity in Cyber Insurance Coverage, 2020,www.oecd.org/finance/insurance/The-Role-of-Public-Policy-and-Regulation-in-Encouraging-Clarity-in-cyber-Insurance-Coverage.pdf, p 5.
20. *Ibid*.
21. *Ibid*.
22. Hurtaud S, *et al.*, Cyber Insurance as One Element of Cyber Risk Management Strategy, 2014, lu-cyber-insurance-cyber-risk-management-strategy-03032015.pdf, *Harvard University, Cost of Data Breach Study: Global Analysis, Ponemon Institute*, p 4. Cyber insurance is written and priced to suit individual customers. As such, insurance policies may stipulate exclusions, impose limits, or add clauses to protect the insurer from higher risks (e.g non-performance of a cloud-computing provider, unencrypted devices that contain personal or other sensitive data, computer software malfunctions due to programming errors).
23. This form of insurance generally covers three types of maritime risk, to wit; ship insurance, cargo insurance and freight insurance. In modern international trade, ship insurance is taken out by the ship owner to cover against loss of a ship resulting from sea perils. Cargo insurance covers goods, produces or merchandised transported by the ship but taken out by the charterer or owner of the goods. Freight insurance covers the risk of loss since freight is payable on delivery of goods in the event of a loss the insurance cover is adequate for restitution integrum or restitution to the status quo ante.
24. Cargo insurance is therefore a section of marine insurance that protects property against loss or damage in the air or sea transit, inland waterways and subsequent land. The aim is the removal of financial burden associated with the damage or loss risk of goods transportation between the importers and the exporters. The insured party gets the right to obtain compensation from the insurer by paying the insurance premium. In this case the losses are repaid by the insurance policy.
25. Emeksiz S, Cargo Insurance for International Business and Transportation *Marine College, State University of New York*, 2012, p 2.
26. The difference is that the total loss contains the actual total loss, the risk loss guaranteed in the policy is guaranteed 100% then the total constructive loss is the value of the loss incurred while transporting the ship is greater than the sum insured. Meanwhile, partial loss contains a particular average which is the value shared with other cargo owners which are calculated from the amount of damage or lost items.
27. Ritonga AI. *et al*, Optimizing the Process of Management of Marine Cargo Insurance Claims at PT. ABC, *Jurnal Logistik Indonesia*, vol. 5, no. 2, (202), p 173.
28. 111 Ohio St.3d 409, 2006-Ohio-5858.
29. In dealing with cargo claims, it is important to remember that international rules apply to the carriage of goods by sea, such as the Hague-Visby, Rotterdam or Hamburg Rules. The legislation to be applied depends on what Rules the particular country has ratified.
30. Trujillo S.K, International Marine Cargo Insurance: Building generic and thematic competences in commercial translation, *The Journal of Specialized Translation*,2019:32:268.
31. *Ibid*, p 269.

32. *Ibid*.
33. *Ibid*.
34. Kumbhakar D, *et al.* An Optimal and Efficient Data Security Technique through Crypto-stegano for E-commerce, *Multimedia Tools and Applications*,2019:82:21006.
35. OECD Joint OECD-Private Sector Workshop on Electronic Authentication, 1999, available at http://www.oecd.org//dsti/sti/it/secur/act/wksp-auth.htm, accessed 16/05/24.
36. Murphy D, The Role of Cryptography in Security for Electronic Commerce, *The ITB Journal*,2001:2(1):26.
37. Dixit PP. Conceptualizing Interaction between Cryptography and Law, *NUJS Law Review*,2018:11(3):327.
38. Section 4(31) of the Cameroon Cyber Law of, 2010.
39. Dixit PP, *op. cit*, p 327.
40. Ghanima S.S and Mishall A. Z, Securing Transactions Using Hybrid Cryptography in E-commerce Apps, *Journal of Education for Pure Science*, vol. 13, no. 3, 2023, p 32.
41. Al-Shabi MA, A Survey on Symmetric and Asymmetric Cryptography Algorithms in Information Security, *International Journal of Scientific and Research Publications*,2019:9(3):577.
42. Venkateshwaran G, Cryptography for Enabling E-Commerce, *Indian Journal of Applied Research*,2016:6(1):621.
43. *Ibid*.
44. Dixit P.P, *op. cit*, p 330.
45. Suguna S, *et al.* A Study on Symmetric and Asymmetric Key Encryption Algorithms, *International Research Journal of Engineering and Technology* (IRJET),2016:3(4):29.
46. Aung MA, Wai MS. Study on Symmetric and Asymmetric Cryptographic Techniques, Meral Portal, University of Computer Studies, Mandalay, 2015. 196. Dixit P.P, *op. cit*, p 331.
47. Sangeetha V. E-commerce with Security Techniques of Visual Cryptography and Text Based Steganography, *International Journal of Arts, Science and Humanities*,2018:6(1):130.
48. Dipesh V, *et al*. "Visual Cryptography: A Review" *International Journal of Computer Applications*,2017:174(5):41.
49. Guru Prasad MB, Nayana GB. Design and Implementation of Visual Cryptography System for Transmission of Secure Data, *International Journal on Recent and Innovation Trends in Computing and Communication*,2017:5(7):718.