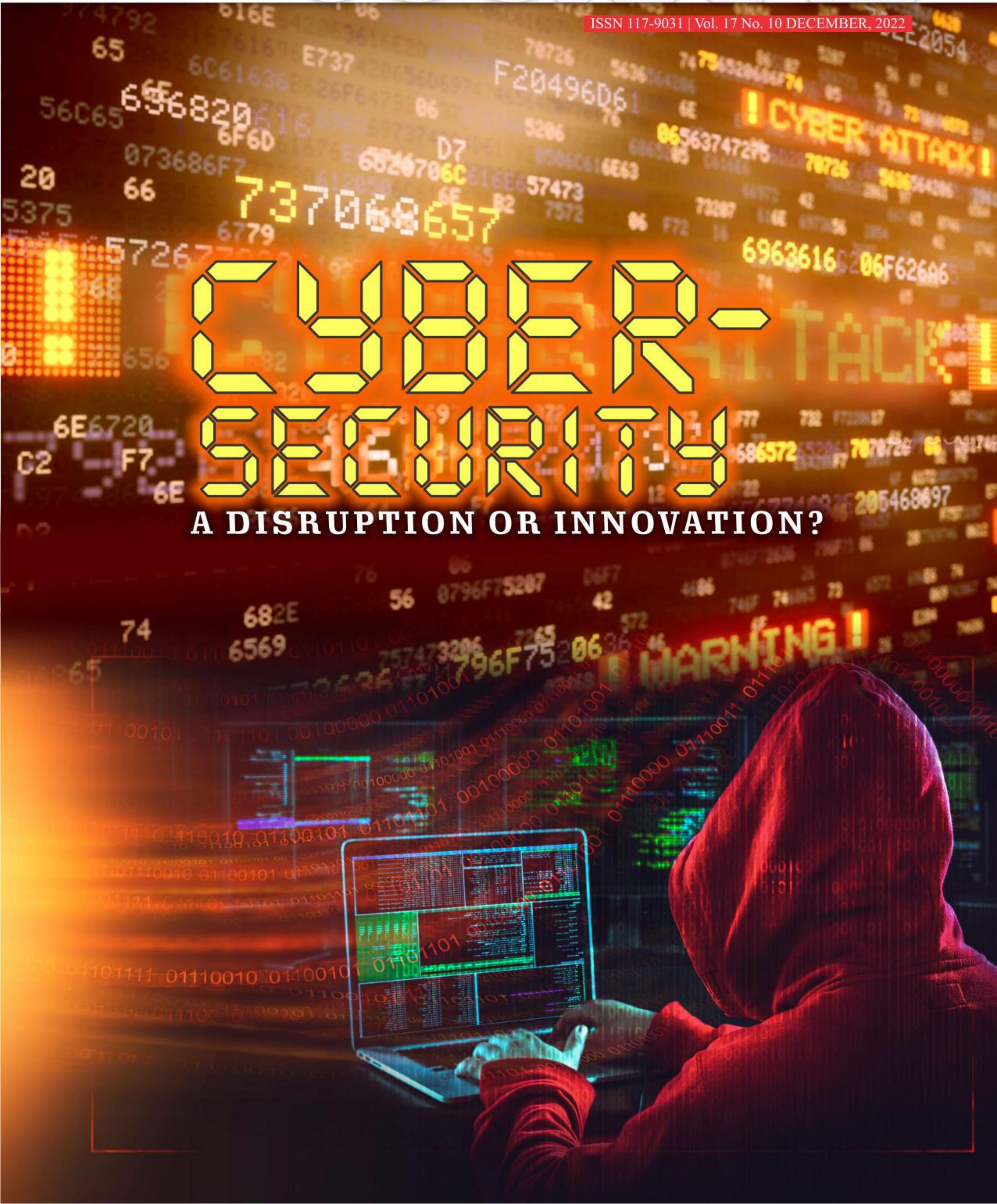
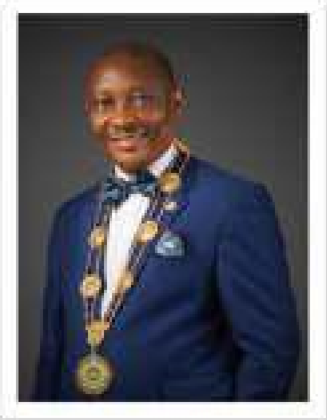
CHARTERED INSURANCE INSTITUTE OF NIGERIA
JOURNAL
ISSN 117-9031 | Vol. 17 No. 10 DECEMBER, 2022



CYBER-SECURITY

A DISRUPTION OR INNOVATION?

Stability
assured
Strength
sustained



From the desk of the President

Welcome to the second edition of our Prestigious Institute's bi-annual Journal publication. It is with a glad heart I convey our best wishes to you our eminent stakeholders, in appreciation of your commendable efforts towards the growth of the Institute and the Insurance Industry at large.

This platform affords me another great opportunity to express my profound gratitude to all members of the Institute, stakeholders of the insurance industry, financial services sector and well wishers for their immeasurable support during my investiture ceremony as the 51st President/Chairman of Council of our great Institute. I was deeply honoured and I pledge to serve the Institute to the best of my abilities and move it to lofty heights.

The world is currently operating in the spheres of vast volatile, uncertain, complex and ambiguous (VUCA) environment and this has tremendously caused paradigm shifts to the operations and processes of businesses across all sectors, with the insurance sector being at the front burners. In all these uncertainties, I must say that the insurance industry has remained dogged with the adoption of digitalisation to effectively process its modus operandi.

Technological innovations and disruptions are continually redefining the wants, needs and expectations of customers and insurance companies consequently, have been tasked to be at the top of their game in this dynamic world. Technology has opened up several opportunities and threats in the form of platforms such as; Artificial Intelligence (AI) Big Data, Block Chain and much more which both serve positive and negative impacts on business operations to the insurance industry and its clients respectively.

It is against this backdrop that this edition focuses on "Cybersecurity: A Disruption of Innovation?", a theme that beams the light on the essence of cybersecurity insurance to organisations, individuals, industries and the need for the insurance industry to strengthen its cyber risks policies and protocols in order to protect its data from malicious attacks online.

The continuous advancement in digital technologies have made it mandatory for organisations as well as individuals to leverage the internet daily for business transactions. It is worthy to note that these disruptions emerge with the positives and negatives and our responses to these will determine the future of our industry. This simply means that as stakeholders, we must continue to be at the frontiers of these technological innovations and trends in the industry; in order to thrive in our endeavours. However, we must keep measuring their advantages and disadvantages to the development of the industry.

It is against this framework that the theme and focus of my Presidency is pinned on "BUILDING A SUSTAINABLE LEGACY". The choice of this theme was borne out of the need for continuity and sustainability of the Institute's accomplishments from my predecessors. This will guarantee that despite current global uncertainties, the Institute will continue to meet the needs and aspirations of its members.

Against this backdrop, we are going to unlock the potentials of this approach by focusing on a three-point agenda:

1. Digital Reinforcement of Institute's Operations.

2. Insurance Awareness for all – Grassroot, Youths and Insuring Public.

3. Infrastructural Development.

Indeed, efforts have been made by my predecessors to revamp the digital operations of the Institute. However, we need to continuously upgrade and innovate our processes to deliver excellent customer experiences and members' satisfaction.

My projection is that my tenure as President of our great Institute will facilitate the transformation of the Secretariat with the state-of-the-art facilities that would stimulate digital operations and processes, enhance excellent work culture which results in quality customer experiences in all our deliverables. Smart Technologies and digital solutions would be deployed to achieve this together with a viable business model.

On insurance awareness creation, our goal is to make insurance attractive to the younger generation. Yes, we want to catch them young and that is why we advise all insurance companies and organisations to adopt secondary schools and educate them on insurance and its values. The Institute has adopted several schools and is currently educating them with secondary school insurance textbooks. In addition, the Institute has many programmes in place aimed at creating insurance awareness and training members to be world class insurance professionals.

These are a few of the many impactful projects we are working on to operate through the Institute and the College of Insurance and Financial Management so as to expand the insurance profession. To achieve these laudable feats, requires teamwork and effective collaborations, hence, I appeal to all stakeholders in the industry to support us in making these plans a success.

I will like to restate that the membership of the Institute is one of the key ways to get to the pinnacle of the insurance profession. You can only pride yourself as a true member of the Institute by posting your dues, levies and actively participating in the programmes outlined in the Institute's calendar. The Institute remains committed to offering value to its members and will continue to improve on its operations to achieve excellence.

As stakeholders of the Institute, the onus is on us to embrace professionalism and uphold the Institute's ethics and values in the course of all our business endeavours. The Institute is our pride and it serves as a guiding light for the insurance industry.

My deepest appreciation once again to you, even as I urge you to continue supporting the Institute as partners in progress to the growth of the insurance industry. We should equally sustain the tempo of excellence that the Institute has been noted for and turn all perceived challenges to steeping stones for greatness.

Have a pleasant reading.

Yours in Service,

Mr. Edwin Igbiti, ACII, FIIN
President/Chairman of Council
Chartered Insurance Institute of Nigeria.

CHARTERED INSURANCE INSTITUTE OF NIGERIA
JOURNAL
ISSN 117-9031 | Vol. 17 No.10 December, 2022

Editor-in-Chief
Mrs. Abimbola Tiamiyu, M.A.S, M.Sc, FIIN

Contributors
Mr. Edwin Igbiti
Peter Offiong
Dr. Folayo Aina
Tobi Osanaiye
Opeyemi Ismail Akintola
Mr. Tope Smart
Vera Aimufua
Osanaiye Olutoyin Adegoke
Obinna Chilekezi & Margaret Jinadu
Emmanuel Chilaka
Samuel Mbonu

Concept, Design & Production
BBM Adarson
Tel:+234 802 976 2850, info@bbmadarson.com

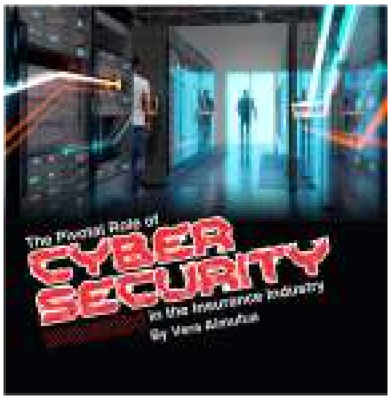
All enquiries should be directed to
CHARTERED INSURANCE INSTITUTE OF NIGERIA
27, Lagos Street, Ebute-Metta, Lagos.
Tel: +234 817 204 0914, +234 909 198 8252
E-mail: info@ciinigeria.org

//////////DISCLAIMER//////////////////////////

All articles in this journal reflect personal opinions and views of the writers rather than that of the Institute.

CONTENTS

36



The Pivotal Role of CYBER SECURITY in the Insurance Industry

By Vera Akinufua

40

CYBER SECURITY and Insurance Solutions

Oyaniyi Olubunmi Adegoke

[illegible]

44

CYBER-SECURITY A DISRUPTION OR INNOVATION IN THE INSURANCE INDUSTRY?

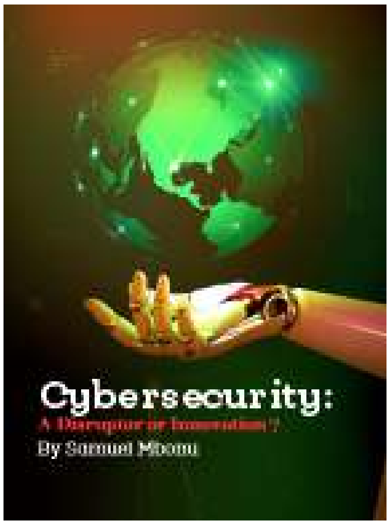
By Obiama Chibikel, [illegible] and Margaret Nwadu, [illegible]

49

HOW CYBER SECURITY IMPACT THE INSURANCE INDUSTRY By Emmanuel Chiluka

IT Department, [illegible]

52



Cybersecurity: A Disruptor or Innovation?

By Samuel Mbonu

INTERSECTION OF CYBER-SECURITY

AND INSURANCE UNDERWRITING INFORMATION

By Peter Offiong FIIN, ACIB, ACA, Msc,
Chairman, Offices Representatives Committee (ORC), CIIN and
the Head of Financial & Professional Services at Scib Nigeria & Company Limited.

OVERVIEW

The cyber threat to businesses is at an all-time high and continues to evolve with many becoming prime targets for global cyber criminals. Headline cyber-attacks between January 2020 and July 2022 continues to highlight the significance of these risks. With such a reliance on technology in order to be connected at all times and conduct work effectively, cyber risks have become a top-of-mind issue. Businesses can no longer rely on traditional insurance coverage in this space and must take a high-level, holistic approach to how they develop their operations to promote a cyber-resilient culture.

Businesses are continuously looking to any margin improving efficiency. This often means the solutions are heavily reliant on technology and digital integration. As a result any loss of internet connectivity will have a significant impact on business operation. While an enhanced understanding of the cyber risk landscape has prompted organisations to spend more on their ICT security, actual take-up of cyber policies still remains relatively low. Those companies operating in the financial/professional services sector have been the most active when it comes to the uptake of cyber insurance or would I say the discussions thereof. They naturally host some of the world's most sensitive data, making it extremely attractive and the obvious choice for cyber criminals to target. However, with the management of data and dependency on technology often a secondary concern for the majority of businesses, the benefit of a cyber policy in helping a business respond to, and recover from, an attack or data breach could prove to be invaluable and must not be ignored. Recent cyber events have had one positive effect, in that they have made organisations much more aware of the cyber risks they face and more conscious of the need to manage their cybersecurity exposure. In spite of this, many companies still struggle to translate their cybersecurity concerns into concrete action.

Cyber insurance is part of a range of tools available to organisations to build up their cybersecurity and resilience. The solutions typically offered by insurers include not only insurance coverage, but also prevention advice and mitigation support in the event of a cyber related incident.

Despite the increasing importance of cyber risks, the market for cyber insurance in Nigeria is still at its infancy. One reason is that cyber risks can be challenging for insurers to cover due to the difficulty in quantifying risks that are constantly evolving and can rapidly spread worldwide. Similarly, organisations can find it hard to accurately assess their cybersecurity exposures and how best to use insurance to mitigate them. The communication of the cyber security maturity level in such a way that the insurer is comfortable enough to underwrite, is very crucial. The other issue bothers on product knowledge on the part of practitioners as well as regulatory issues around product approvals. However, these challenges have not prevented insurers and brokers from developing solutions, and the market is evolving rapidly.

Despite the increasing importance of cyber risks, the market for cyber insurance in Nigeria is still at its infancy. One reason is that cyber risks can be challenging for insurers to cover due to the difficulty in quantifying risks that are constantly evolving and can rapidly spread worldwide.

The insurance solutions proposed often reflects an organisation's cyber risks journey. These are not uniform and depend on the organisation's characteristics, including its size, type, sector and level of digitalisation. Large organisations tend to rely on tailor-made cyber insurance solutions targeted at their needs. Small organisations meanwhile, can opt for one of a range of standardised cyber insurance products. On the other hand, their size and operations might not be adequately addressed by a standardised product. They may not have the necessary resources within the organisation to undertake a comprehensive cyber risk assessment to gauge whether they need a tailor-made solution. Whatever the situation, a key component of success in any cyber insurance deal is a good understanding between the potential insured, their broker and the insurer.

In the end, the insurer must be fortified to not only face the risks of cyber-attack as an organisation but to provide immediate and long-term solutions to clients when the risks occur. Going through this journey requires a thorough understanding of the cyber underwriting information as well as the ability to interpret this information for better underwriting. This is a skill that is often neglected but critical to the cyber insurance journey.

UNDERSTANDING CYBER UNDERWRITING INFORMATION

Whether an organisation is buying cyber insurance or selling, there are critical questions they must face and confront. This information can help businesses of all sizes and across all sectors better manage their cybersecurity risks. There is generally a common thread in the type of information insurers will ask an organisation to provide during the cyber insurance discussion. This part of the process is very important for both sides. The insurer will rely on this information for underwriting purposes, as well as to offer related services. Meanwhile, the potential

insurance buyer will be able to assess their cybersecurity needs, and to identify the people to involve in the event of a cyber-related incident. The broker will equally play a crucial role in this dialogue, confirming that the potential buyer has a good understanding of their cyber risks and of the insurance options. An effective discussion on cyber insurance, based on a high level of understanding between an insurer/broker and the prospective insured, is essential to tackle cyber risks effectively. Collecting appropriate internal information can play a huge role in achieving this. Typical underwriting information would include the following:

General Business Information

The general business information is intended to allow the insurer to understand the extent of the organisation's exposure to cyber threats and to better assess what solution to offer. Typical information would be main activities, sector, type of products and services, claims and third-party losses, geographical area (countries, jurisdictions), information about multiple or single offices and the location of supply chains, production processes and assets (tangible and intangible), turnover, income, IT security budget, etc.

These information would shape the insurer's profile of the insured looking for cyber insurance coverage. It will also help the insurer assess the insured's exposure to potential claims and third-party losses, the governing laws and jurisdictions, the political risks, commitment of the insured to cybersecurity as well as a useful indicator of the risk maturity of the client.

Cybersecurity Corporate Culture

The human component is a critical cybersecurity factor. Since digital transformation affects all the elements of an organisation, the ability of the organisation to raise awareness and train the operational teams, and not only IT people, is an important indicator of the level of development of cybersecurity risk management. The insurer may therefore want to know more about the training of management and operational teams in information system security and control of outsourced services, including documentation.

An insurer could look at whether IT security is a matter for a small group of dedicated persons or a general concern for everyone within the organisation. Each element might indicate the presence of a corporate culture in which IT security is embedded into the training of each user. These indicators could feed into the insurer's general assessment of the organisation and its capacity to prevent damages/losses incurred by employees.

Information System Security

Insurers may ask an insurance buying organisation if there is internal capacity to map all the physical systems inside and outside the organisation, as well as the data/information within these systems. Insurers may be interested to know what this data is and its uses. Important indicators include the ability to identify the most sensitive information and servers. For insurers, the organisation's ability to identify sensitive data and critical equipment is a positive sign that the organisation is engaged in IT security. Insurers may especially value information about:

- Management of critical access to networks, equipment and maintenance.
- Management of all outside access for maintenance purposes with a clear differentiation between access rights.

This is where organisations can demonstrate how access points are controlled, showing the relationship between the access points and the criticality of the information and systems. Showing that measures have been taken to physically secure mobile devices can be helpful. This includes the encryption of sensitive data, in particular on hardware that can be lost. The organisation may also have adopted security policies for the network connection of mobile devices used in mobile working. This can be an indicator of how the risk of data leaks is managed.

> Since digital transformation affects all the elements of an organisation, the ability of the organisation to raise awareness and train the operational teams, and not only IT people, is an important indicator of the level of development of cybersecurity risk management.

Also, having networks accessible within a single space is considered a risk factor for the organisation, so seeing that networks are segmented and partitioned is likely to be a positive indicator for the insurer. An insurer may ask the following questions:

- If and how networks are divided into different zones according to the criticality of the systems to avoid the spread of an attack from a compromised, low-critical system, such as a workstation, to a critical one, such as a server.
- What can be accessed from the outside and/or the internet (for instance, whether the HR and payroll system is accessible from the internet) and whether there is a partition between these areas.
- What security exists for Wi-Fi access networks and whether there are secure network protocols.
- Whether there is a secure access gateway to the internet and if services visible from the internet are segregated from the rest of the information system.
- How secure the dedicated network interconnections with partners are.
- What physical controls protect access to the server rooms and technical areas.
- What levels of redundancy are in place to ensure the availability of information and systems.

Information about these elements gives the insurer an indication of how well the organisation can reduce the risk and mitigate an outage of its networks.

Administration rights are a critical point. If abused, they pose some of the greatest risks. Evidence that these risks are well managed includes:

- Identification of each individual accessing the system by name and distinguishing of the generic user/administrator roles.

- Allocation of the correct rights to the information system's sensitive resources.
- Setting and verification of rules for the choice and size of passwords and protection of passwords stored on systems.
- Changes to the default authentication settings on devices and services and use of a two-factor authentication where possible.
- Prohibition of internet access from devices or servers used by the information system administration.
- Use of a dedicated and separated network for information system administration and limitation of administration rights on workstations to strictly operational needs.

Specific treatment of administration rights reduces the risk of abuse.

IT Suppliers:

Outsourcing IT/cybersecurity-related functions does not remove the responsibility of an organisation for managing the associated risks. The quality and reputation of the IT suppliers could help insurers understand better the risks of accumulation in the case of a cyber attack. It may also be highly relevant for the insurer to know if the organisation has mapped all outsourced cyber activities, with a list of the most relevant IT suppliers, as well as documentation about how outsourcing contracts are written and managed.

IT Update Management

Insurers may ask organisations about their policies for updating the components of their information systems and anticipating software and system end of life/maintenance. The presence of some specific software that cannot be updated and the corresponding controls in place to mitigate vulnerabilities are also relevant information. It might be useful to explain whether this process is centralised and automated or whether it relies on users acting voluntarily, regularly and independently to maintain their systems. The management of updates and obsolescence indicates how well the organisation mitigates threats that exploit vulnerabilities in software and completes the overall picture of the capacity of an organisation to face its cyber risks.

Ongoing Assessment

As cyber attacks are always possible, the organisation should have a systematic approach to

Insurers may ask organisations about their policies for updating the components of their information systems and anticipating software and system end of life/maintenance.

identifying, checking and reviewing its weakest points. It should inform insurers about the cyber risk management guidelines it is following. Beyond its own internal approach, the organisation may also use baseline guidelines such as those recommended by governments or their agencies. Cyber Crime Act of 2015, Nigerian Data Protection Regulation of 2019 as well as the CBN Cybersecurity Framework for Payment Service Providers might be relevant examples for a Nigerian player. Insurers might ask the organisation to explain how it would manage a cyber crisis. Cyber risk management plans can include a crisis management component to prepare the organisation for recovery after an event. As part of this plan, the organisation is likely to be expected to:

- Activate and configure the most important component logs.
- Define and apply a backup policy for critical components.
- Undertake regular checks and security audits, then apply the associated corrective actions.
- Designate a point of contact in information system security and make sure staff are aware of who it is.
- Have a defined security incident management procedure.

Insurers usually want some assurance that there is an internal audit strategy to verify and check that these points are effectively handled with an assessment and measurement of their performance. Crisis management recovery plans are also important because they can directly affect the magnitude of the losses and the organisation's ability to resume activities after an attack.

Personal Data

Insurers may want to assess the extent of exposure to sensitive personal data, in order to understand:

- How much personal data is managed by the insurance buying organisation (health records, credit card records, etc.).
- The origin of these records.
- Where the data is stored and processed.
- Who within the organisation has responsibility for handling this issue.
- What measures are in place to protect against attacks on these databases (encryption, for instance).

Personal data loss can be expensive for an organisation if it has to indemnify clients and third parties, particularly in countries with strong privacy regulations.

CONCLUSION

Cybersecurity is a cross-functional issue whatever the size of an organisation. Senior management will need to involve most functions in preparing for a dialogue on cyber insurance with other market participants. Compiling the information may be demanding (in fact some cyber insurance discussions end abruptly at the point of completing the proposal form. You may never hear from the client again), but also creates a virtuous circle because it allows the organisation to identify where it can strengthen its policies and procedures. Cyber insurance is an evolving market. Detailed information about an organisation and a description of how cyber risks are understood and managed can improve the preparation of the dialogue with insurers and brokers.

Today, organisations of all sizes are striving to address their cyber risks and integrate them into their overall risk management programme. In this respect, cyber insurance can be a useful tool. Preparing the information required by insurers may initially seem daunting, but the rewards are worth the effort. This is because the exercise serves to gauge the extent to which they are ready to face cyber risks generally, both in terms of preventing them and of reacting appropriately should an event occur.

Similarly, on the basis of this information, the insurer will be able to offer the coverage that is best suited to the organisation's needs, and, equally importantly, access to pre-and post-incident services. The cyber insurance landscape is likely to evolve as insurers continue to develop solutions and cyber risks become easier to quantify.

Reference/Credits:

Cyber Liability Insurance Handbook. RPS
Federation of European Risk Management Associations (2018). Preparing for Cyber Insurance.

CYBER-SECURITY: A Necessity for the Insurance Industry

Dr. Folayo Aina
Lecturer at University of Central Lancashire, United Kingdom

Introduction

Insurance companies are adopting digitalisation to achieve more ease of access, automation, effective analysis, and improved processes, etc. The insurance industry is highly dependent on digitalisation to perform its day-to-day operations and deliver services to its customers. Along with this digital transformation, cyber security risk is also involved, especially in small to midsize insurance enterprises.

Cybercriminals know that insurance companies have valuable data and information of their policyholders, which is a gold mine for threat actors. Therefore, insurance companies that are not taking steps to protect against cyber security risks are low-hanging fruits for bad actors.

According to (Potiviti, 2017), there was a noticeable surge in successful cyber-attacks in the insurance industry. Personal data of over 100 million Americans have been compromised in these security breaches. While in the first quarter of 2021, one of the largest insurance companies in the USA, CNA Financial Corporation has paid $40 million as a ransom amount to regain access to their network (Bloomberg.com, 2022). The interest of cybercriminals in the insurance sector is a sign that strict actions are mandatory to mitigate the cyber security risk in the insurance industry.

Why Cybersecurity is Important in the Insurance Industry?

Companies that have the most valuable consumer data are hot targets for cybercriminals. Therefore, cyber security attacks in the insurance sector are increasing exponentially. A successful security breach can cause financial and reputation damage to insurance companies. To avoid this loss, insurance companies must implement cyber security systems to protect themselves from the leakage of confidential data and other security breaches.
The most valuable data insurance companies have is the personal identifications and information of their customers. With the release of the data protection and privacy act, all companies are recommended to keep the customer's data secure and confidential, and if they did not do so, they may face legal proceedings in court and no insurance company wants that.

We have seen in the past, threat actors always try to steal confidential data from insurance companies and sell it on the deep web, use them in insurance fraud, demand ransomware, and blackmailing. No insurance company would want to find its sensitive valuable data stolen, which is why insurance companies need to take steps to make sure that their data is secure from threat actors.
Common Cyber-attacks on the Insurance Industry

- **Ransomware**

According to (SonicWall, 2021) report, there were 304.6 million ransomware attacks in the year 2021. Cybercriminals inject malicious software into the computer system which is designed to restrict user access until the ransom is paid to unblock it.

- **Social engineering**

Another common cyber security threat for the insurance industry is social engineering attacks. Bad actors physiologically trick the concerned employees of the company to gain access to sensitive information. Social engineering attack involves human error. Phishing and impersonation attacks are most common in social engineering attacks.

- **Third party**

Insurance companies are highly vulnerable to third-party attacks when they collaborate with outside third-party networks or vendors to service their customers. Every single time an insurer's network relates to outside their party or vendor network, there is a health risk of any malware injection or supply chain attack (Bloomberg.com, 2022).

How to prevent cyber security attacks in the insurance sector

1. Apply Robust Security Plan

To defend against cyber security risks for insurance companies, a vigorous cyber security plan is needed. Gathering all information about what areas needs to be protected, how much cost it implies, how it will be implemented and checked, what effect does it have on the entire system, and how you will achieve your cyber security metrics and KPIs. Keeping compliance and data privacy regulations in mind and following the NIST cyber security framework can lead you to an effective cyber security system for the insurance business.

2. Apply Zero-Trust Network (ZTN)

A zero-trust network is another effective solution to protect your system. Zero trust means not to trust anyone and always verify. By applying a zero-trust network you are authenticating and authorizing every single attempt to access your network. ZTN will protect your sensitive data by authenticating every user or machine who will try to access it and apply the least privilege to provide less access.

3. Firewall/Encryption and Backups

These three actions must be part of regular routine in cyber security practice. The security system will protect your network and monitor incoming and outgoing traffic and decide whether to allow it or not based on the principles you set. A security system is essential when communicating with a third party or vendor. Always keep your valuable data encrypted, because, in case of any threat actor accessing it, they will only get gibberish-looking text instead of actual sensible data. Lastly, daily backup is compulsory in insurance companies because data is added, modified, and deleted with high frequency in insurance companies on daily basis, so it is a clever move to take backup every day. Daily backup can save you millions of dollars in case of a ransomware attack.

- **Monitor and Test Security Performance**

Keeping track of how well your security system is performing is a key to improving your cyber security for an insurance company. You must monitor and analyse your cyber security performance according to the matrices and KPIs you have set. Additionally, testing your security system from time to time is a wise decision to check if it is securing your parameter properly. Monitoring and testing will let you know the reliability of your cyber security system.

Case study of Anthem Insurance Companies, Inc.
The data security breach of Anthem's systems in late January 2015 potentially exposed the personal records of around 78.8 million customers (Commerce. Alaska, 2022) Anthem paid out $260m (anthem, 2022) for security improvements and remediation, and a further $115m (Insurance.ca.gov, 2022). in June 2017 to settle lawsuits from customers potentially affected.

What happened?

On 27 January 2015, Anthem Insurance Companies, Inc discovered a major data security breach. Anthem is the largest health benefits company by membership in the United States, with member insurers licensed to conduct business in all 50 states and the District of Columbia. The breach was eventually thought to have potentially exposed the records of around 78.8 million customers. Data affected reportedly included names, birthdays, social security numbers, addresses and email addresses, as well as employee information, but not credit card or medical data. Anthem immediately alerted its principal regulator as well as the FBI, and called in a firm of consultants to help it assess remediation steps required.

- Immediate costs: Very high

The costs of the incident have been truly considerable for Anthem. The initial cost of security improvements, remediation and clean up after the breach have been estimated at $260m (Insurance.ca.gov, 2022). This is despite the fact that there is reportedly no evidence to date that any customer data has been bought or sold on the dark-net by cyber criminals. Indeed, this has led some observers to speculate that the attack could have been initiated by a nation state rather than a cybercrime gang. The California Department of Insurance said it had a "medium degree of confidence" that the attacker was affiliated with a foreign nation state (info security, 2022).

- Slow-burn costs: High

In addition to these immediate costs, Anthem also faced a very stiff bill for the slow-burn effects. In late June 2017, it was announced that the insurer would be paying $115m to settle litigation stemming from the attack. This settlement, at the time of writing, is still subject to the approval of the presiding US district judge (anthem, 2022). The money will be used to pay for two years of credit monitoring for those potentially affected by the attack (Insurance.ca.gov, 2022). That is in addition to an initial two years of credit monitoring already offered by Anthem. Web attacks are the biggest risk for retailers, as they target firms that offer rich digital services to clients.

Where from here?

KPMG suggests that insurers should focus on five key areas to address cyber risks.

- Ownership: Cyber security is a business issue, not an IT issue. Some of the more successful insurers have elevated their Chief Security Officer to report directly to the Chief Operating Officer, creating clear line of sight between the business and the risk.
- Capabilities: New and improved cyber security capabilities are likely to be required. But insurers will also want to assess their current 'pockets' of cyber security excellence and ensure those best practices are shared across the enterprise. Leading insurers are starting by ensuring that their existing capabilities are being properly utilised.
- Awareness: Improved awareness from the C-level down is key. Insurers need to focus on improving their understanding of their ecosystem of third-party participants – non-affiliated agents, outsourced service providers and other non-employees with access to data – to manage their risk in a consistent manner.
- Organisation: Chief Executive Officers will need to work with their business leaders to understand the right balance of centralised and decentralised services to meet the cyber risks most appropriately in each market. Creating the right structure for robust and consistent cyber security is key to fielding a responsible (and defendable) response.
- Preparedness: Successfully activating a response and recovery programme takes practice, commitment, and clear lines of responsibility. From 'red teaming' exercises that simulate the way attackers behave through to improved employee training and more frequent drills, insurance leaders need to carefully consider how to ensure their organisation remains prepared.

Conclusion

The significance of cyber security risks in the insurance business can be seen by the epidemic growth of security breaches in the insurance sector. Cyber-attacks can cause insurance companies heavy financial loss, reputation damage, and can lead them to court cases for not protecting the confidential information of policyholders.
Therefore, insurance companies must take immediate action to implement robust cyber security plans which is able to prevent user personal data and the most common attacks happening in the insurance industry.

References

1.https://www.protiviti.com/sites/default/files/united_states/insights/cybersecurity-regulatory-issues-in-the-insurance-industry-protiviti.

2.https://cdw-prod.adobecqms.net/content/dam/cdw/on-domain-cdw/brands/sonicwall/sonicwall-2021-cyber-threat-report.pdf

3.https://www.commerce.alaska.gov/web/Portals/11/Pub/Companies/Exams/MCE16-09.pdf?ver=2016-12-12-083253-927

4. http://www.insurance.ca.gov/0400-news/0100-press-releases/2016/upload/Fully-Executed-RSA-2.PDF

5. https://anthemdatabreachlitigation.girardgibbs.com/wp-content/uploads/2017/06/2017-0623-Dkt-869-8-Settlement-Agreement.pdf

6. http://www.insurance.ca.gov/0400-news/0100-press-releses/2016/upload/Fully-Executed-RSA-2.PDF

7. https://www.infosecurity-magazine.com/ne ws/anthem-to-fork-out-115m-in-breach/

8. https://anthemdatabreachlitigation.girardgibbs.com/wp-content/uploads/2017/06/2017-0623-Dkt-869-8-Settlement-Agreement.pdf

9. http://www.reuters.com/article/us-anthem-cyber-settlement-idUSKBN19E2M

CYBER RISKS:

IMPLICATION FOR THE INSURANCE INDUSTRY

By Tobi Osanaiye
President, YIPs Africa

Introduction

In 2020, the world ostensibly entered a new era of cyberattacks. Although, over the years, various forms of breaches, viruses, and other forms of attacks have existed, but research has it that there was a drastic rise in the propensity to pay ransomware cases recently thereby bringing forth a wider swath of geopolitical circumstances that hackers have found favourable.

The Covid 19 pandemic has accelerated digital transformation because most organisations have increased their use of information technology. They are more prone to relying on digital and remote solutions to perform their daily activities while delivering services to their customers. While this has brought along advantages, the growing reliance on digital solutions has also increased the risk of cyber-attacks.

Cyber risks are regarded as a top global risks for the economy and financial sector as a whole. The various ICT exposures have not changed over the years and people still find themselves undertaking the same process over and over again which keeps them exposed thereby resulting in a high frequency of incidents.

What is Cybersecurity Insurance?

Cybersecurity insurance safeguard businesses against financial losses instigated by cyber incidents, including theft and data breaches, system hacking, denial of service, and ransomware extortion payments. For small businesses that store sensitive information on a computer or online, this coverage could prove useful.

The outrageous aspect of the perpetrators is that they constantly develop new ways of infiltrating their acts which makes it very difficult for law enforcement agencies and security operatives to keep up.

This new reality is putting much pressure on the insurance industry to figure out ways to handle the risk and how best to protect organisations and businesses from a potentially catastrophic breach.

Relationship between Cyber Risk and Insurance

The transformation of organisational activity to ICT-inclined operations has led to an increase in the market of cyber risk underwriting. According to statistics, the cyber insurance market is anticipated to grow exponentially between 2020 and 2030. Therefore, insurers have a critical role to play in putting together drastic measures in mitigating such risks.

As a consequence of the digitalisation of the economy, it cannot be overemphasised that cyber risk has been gaining increasing relevance thereby becoming one of the main operational risks encountered by organisations.

The increasing sophistication and frequency of cyber-attacks and the continuous digital transformation have also made insurers increasingly susceptible to cyber threats, as increasingly insurance undertakings are embracing new technologies and making use of big data.

Cyber Risks Challenges Posed on the Insurance Industry

The digital age is upon the insurance industry and the industry is left with no other option than to embrace the challenges that come with cyber risks thereby safeguarding people against the accelerated impact of cybercrime which can be both astronomical and extremely difficult to quantify.

The cyber security insurance landscape is believed to be faced by the ever-changing nature of hacking strategies. This has been illustrated by numerous high-profile examples of cyber-attacks on organisations such as the FBI, Anthem, Uber, Equifax, Target, NSA, and many more corporate organisations thereby making the threat very urgent with high stakes embedded in it. It is quite unclear the level of coverage that the named companies have had against this cyber nightmare, but the crippling attack illustrates the phenomenally high stakes involved. In today's world which is fraught with unimaginable risks, cyber security insurance is fast becoming a necessity to guide against the dark world of online evildoers.

CYBER SECURITY
RISK ANALYSIS

century threat has itself become a sort-out industry, as organisations and corporations around the world ramp up their defenses by hiring skilled cyber security professionals and putting a high-tech system in place.

Analysis of the Threats, Opportunities, and Issues of Cyber Security in the Insurance Industry

Threat: Protecting Insurers and Brokers from Attacks

Insurance companies, agents, brokers, adjusters and other parties involved in property and casualty insurance make vast use of the Internet and digital technology to serve the risk management needs around the globe. The digital age has brought about extensive benefits for the insurance industry and its customers but has also introduced substantial risks. Most especially, the risk of malicious cyber-attacks continues to grow in complexity and severity. The volume and nature of the attacks continue to escalate and evolve, representing a threat to society at large, including the daily activities of the insurance industry. There is a rising understanding that disruptions will be faced even with the best protective efforts, and it is necessary for everyone involved in the insurance industry to plan for how to reduce the consequences of cyber-attacks. The insurance industry can and must do more to protect itself and its customers.

Opportunities: A Growing Market for Cyber

Insurance

The cyber insurance market is quite new and therefore being misunderstood in comparison to other lines of business. Cyber risk coverage is recognised as higher risk than established lines because there is a lack of historical experience and an ever-changing type of cyber-attacks. Commercial cyber coverage varies significantly in availability and form between insurers. As far back as the 1990s, most insurers have been working to remove cyber risks from basic commercial liability and property coverage and introducing a package policy or standalone cyber coverage. For insurance companies providing cyber insurance, coverage is shifting to offer a broader spectrum of protection against the theft, loss, or destruction of a company's digital assets. This coverage can therefore extend to supply chain disruption and business interruption thereby providing immediate and paid access to an incident-response team. The growing acceptance of cyber insurance by businesses as an effective risk transfer solution cannot be overemphasised across the globe today. Coverage for fraud and identity theft is offered at the individual level, as an optional endorsement or it can be included in basic coverage for homeowners and tenants.

Issue: The Uncertain Role of Insurance in a Policy

Insurance consumers and policymakers seem to be greatly unaware of the identity and fraud protection that is available from personal lines insurers. Cyber experts, Cyber security policymakers, and consumer advocates appear unfamiliar with the existence of cyber insurance coverage that is available to both large and small businesses. Moreover, most of the cyber losses are presently uninsured. Insurance is the business of managing and mitigating risk; however, they have the potential to play a much larger role in society's management of cyber threats. Insurance is therefore an essential part of how people tend to manage the risk of vehicle damage through either collision or fire. Also, insurance is recognised as critical for managing the risk of physical damage from seismic risks, floods, and climate. Policymakers' perspective on the role of insurance in cyber risk management is quite uncertain amidst the current cyber security policy conversation.

Conclusion

The future is already upon the insurance industry with respect to the cyber environment and it is very delicate, given the combination of recent losses, threat volatility, and a nascent commitment that could be withdrawn or reduced by the insurers in the space. A wave of cyberattacks with enormous insurance industry implications would not likely pose a solvency threat, but a worst-case situation coming to pass could result in structural shifts to the cyber class of business or even an insurance industry that is just a lot less concerned in cyber. That could possibly result in an important risk management operationalisation with significant technology exposure targeted at most major and mid-sized companies.

References

Beazley. "2019 Breach Briefing." NCSC, 2019.

Laux, Jon and Craig Kerman. "Cyber Update: 2016 Cyber Insurance Profits and
Performance." Aon Benfield, 2017.

Moren, Harry, Russell Cohen, and Aravind Swaminathan. "Does Your Insurance Cover
Phishing Attacks and Business Email Compromise? The Uncertainty Continues..." Orrick
Trust Anchor, 2 November 2016.

Morgan, Steve. "2019 Official Annual Cybercrime Report." Herjavec Group, 2019.

Munich Re. "Demand for cyber insurance growing rapidly: Munich Re offers more than just insurance." Munich Re, 22 October 2018.

Norton. "Cyber Safety Insights Report Global Results." Norton, 2019.

Pascual, Al, Kyle Marchini, and Sarah Miller. "2018 Identity Fraud: Fraud Enters a New Era of Complexity." Javelin, 2018.

AN OVERVIEW OF CYBERSECURITY: CHALLENGES AND ITS EMERGING TRENDS

By Opeyemi Ismail Akintola
Property & Casualty Portfolio Manager at AXA Mansard Insurance

Introduction

Every day, all around the world, thousands of Information Technology (IT) systems are compromised. Some are attacked purely for the kudos of doing so, others for political motives, but most commonly they are attacked to steal money or commercial secrets.

The belief that "it will not affect us" is one of the biggest blunders a modern-day organisation can make on the issue of cybersecurity. The cybersecurity threat is real, and it is, now, a worldwide problem.

In this digital and cloud era, every organisation, be it SMEs or large and multi-national corporations, governments, or banks and financial institutions, faces the threat of a system hack, ransomware attack, data breach, or malware. Cyber-criminals of today are not old-time lone hackers. They run organised crime networks and often operate like start-up companies, hiring highly trained programmers to innovate new online attacks.

The internet penetration globally is estimated at about 3.4 billion users (approximately 46% of the world's population), opportunities for cybercrime have ballooned exponentially. Combating this is multi-disciplinary affair that spans hardware and software through to policy and people with all of it aimed at both preventing cybercrime occurring in the first place or minimising its impact when it does. This is the practice of cybersecurity.

An important clear factor is; it's only going to increase. As we integrate technology further into our lives, the opportunities for abuse grows. So then, we must employ the defences to stop them through the education and practice of cybersecurity.

> These days all small, medium, and large companies are slowly adopting cloud services. In other words, the world is slowly moving towards the clouds.

What is Cybersecurity?

Just as with any technological advancement throughout history, whenever new opportunities are created, there will always be those that exploit them for their own gains. Securing information have become one of the biggest challenges in the present day. Whenever we think about cybersecurity the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day and it involves activities such as bringing down websites, stealing data, or committing fraud.

Cybersecurity is a set of processes, technologies, and methods to protect servers, computers, networks, electronic systems, data, and mobile devices from unauthorised access through malicious attacks. Securing the availability, confidentiality, and integrity of an organisation's digital assets and software against internal or external threats is the primary objective of cybersecurity.

Why Cybersecurity?

The range of operations of cybersecurity involves protecting information and systems from major cyber threats. These threats take many forms. As a result, keeping pace with cybersecurity strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people (Seemma, Nandhini and Sowmiya 2018). Some of the common threats are:

Cyber Terrorism: It is the innovative use of information technology by terrorist groups to further their political agenda. It took the form of attacks on networks, computer systems and telecommunication infrastructures.

Cyber Warfare: It involves nation-states using information technology to go through another nation's networks to cause damage. In the U.S. and many other places in a society, cyber warfare has been acknowledged as the fifth domain of warfare. Cyber warfare attacks are primarily executed by hackers who are well-trained in the use of benefitting the quality of details of computer networks, and operates under the favourable support of nation-states. Rather than closing a target's key networks, a cyber-warfare attack may force a situation into networks to compromise valuable data, degrade communications, impair such infrastructural services as transportation and medical services, or interrupt commerce.

Cyber Spionage: It is the practice of using information technology to obtain secret information without permission from its owners or holders. It is the most often used to gain strategic, economic, military advantage, and is conducted using cracking techniques and malwares.

Who are Cyber Criminals?

Cyber criminals are those who conduct such activities as child printed sexual organs or activity;

credit card fraud; cyber stalking; defaming another online; gaining unauthorised access to computer systems; ignoring copyright, software licensing and trademark safe to protect; overriding encryption to make illegal copies; software piracy and stealing another's identity to perform criminal acts. They can be categorized into three groups that reflect their motivation using the works of Seemma, Nandhini and Sowmiya (2018)

Type 1: Cyber Criminals – Hungry for recognition: These are hobby hackers, IT professionals (social engineering is one of the biggest threats), politically motivated hackers, terrorist organisations.

Type 2: Cyber Criminals – Not interested in recognition: They are psychological hackers, financially motivated hackers (corporate espionage). state – sponsored hacking (national espionage, sabotage) and organised criminals.

Type 3: Cyber Criminals – The insiders: These are former employees seeking revenge, competing companies using employees to gain economic advantage through damage and/or theft.

Many players pose a risk to information

Those who pose as a risk to business information assets are:

Cybercriminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their own companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees or those who have legitimate access, either by accident or deliberate misuse.

The threat is not only technical

Many attempts to compromise information involve what is known as social engineering, or the skillful manipulation of people and human nature. It is often easier to trick someone into clicking on a malicious link in an email that they think it is from a friend or colleague than it is to hack into a system, particularly if the recipient of the email is busy or distracted. And there are many well documented cases of hackers persuading IT support staff to open up areas of a network or reset passwords, simply by masquerading as someone else over the phone.

The key is effective enterprise-wide risk management and awareness

Being aware of potential threats is a normal part of risk management across the private sector. Alongside financial, legal, HR and other business risks, companies need to consider what could threaten their critical information assets and what the impact would be if those assets were compromised in some way. The key is mitigating the majority of risks to critical information assets and being able to reduce the impact of and recover from problems as they arise.

Types of Cybersecurity Threats

The use of keeping up with new technologies, security trends and threat intelligence is a challenging task. However, it should be in order to protect information and other assets from cyber threats, which take many forms which includes the following:

Ransom ware; a type of malware that involves an attacker locking the victim's computer system files typically through encryption and demanding a payment to decrypt and unlock them.
Malware; any file or programme used to harm a computer user, such as worms, computer viruses, Trojan horses, and spyware.
Social engineering; an attack that relies on human interaction to trick users into breaking security procedures in order to gain sensitive information that is typically protected.
Phishing; a form of fraud where fraudulent emails are sent that resemble emails from reputable sources; however, the intention of these emails is to steal sensitive data, such as credit card or login information.

Trends Changing Cybersecurity

Below are some of the main trends that are changing and impacting cybersecurity:

Webservers

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they have compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall a prey to these crimes.

Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks, security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cybercrimes, a lot of care must be taken in case of their security issues.

APT's and Targeted Attacks

APT (Advanced Persistent Threat) is a whole new level of cybercrime ware. For years, network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve security techniques in order to prevent more threats coming in the future.

IPv6; New Internet Protocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cybercrime.

Cloud Computing and its Services

These days all small, medium, and large companies are slowly adopting cloud services. In other words, the world is slowly moving towards the clouds. This latest trend presents a big challenge for cybersecurity, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities, but it should always be noted that as the cloud evolves so also, its security concerns increase.

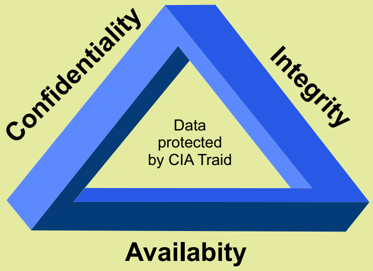
Encryption of the Code

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. Additional use of encryption obtains more problems in cybersecurity.

Internet of Things and Big Data

With the emergence of the Internet of Things (IoT), there is a lot more data to manage and secure. IoT is a large network of physical objects, such as sensors and equipment that extend beyond the traditional computer network. All these connections, plus the fact that we have expanded storage capacity and storage services through the cloud and virtualisation, lead to the exponential growth of data. This data has created a new area of interest in technology and business called "Big Data". With the velocity, volume, and variety of data generated by the IoT and the daily operations of business, the confidentiality, integrity, and availability of this data is vital to the survival of an organisation.

Confidentiality, Integrity, and Availability



In order to efficiently succeed in the implementation of cybersecurity, attention must be geared towards Confidentiality, Integrity, and Availability, known as the CIA triad, which is a guideline for information security for an organisation. Extract of extant literature from Netacad (Cisco Network Academy) postulates that confidentiality ensures the privacy of data by restricting access through authentication encryption. Integrity assures that the information is accurate and trustworthy. Availability ensures that the information is accessible to authorised people.

Confidentiality

Another term for confidentiality would be privacy. Company policies should restrict access to information to authorised personnel and ensure that only those authorised individuals view this data. The data may be compartmentalised according to the security or sensitivity level of the information. For example, a Java programme developer should not have to access to the personal information of all employees. Furthermore, employees should receive training to understand the best practices in safeguarding sensitive information to protect themselves and the company from attacks. Methods to ensure confidentiality include data encryption, username ID and password, two factor authentication, and minimising exposure of sensitive information.

Integrity

Integrity is accuracy, consistency, and trustworthiness of the data during its entire life cycle. Data must be unaltered during transit and not changed by unauthorised entities. File permissions and user access control can prevent unauthorised access. Version control can be used to prevent accidental changes by authorised users. Backups must be available to restore any corrupted data.

To provide reliable services to IoT users, integrity is a mandatory security property in most cases. Different systems in IoT have various integrity requirements. For instance, a remote patient monitoring system will have high integrity checking against random errors due to information sensitivities. Loss or manipulation of data may occur due to communication, potentially causing loss of human lives.

Availability

Maintaining equipment, performing hardware repairs, keeping operating systems and software up to date, and creating backups ensure the availability of the network and data to the authorised users. Plans should be in place to recover quickly from natural or man-made disasters. Security equipment or software, such as firewalls, guard against downtime due to attacks such as Denial of Service (DoS). Denial of service occurs when an attacker attempts to overwhelm resources, so the services are not available to the users.

Steps to Reduce Cyber Risk

The CESG the Information Security Arm of GCHQ - GCHQ, BIS and CPNI In its publication in 2012 stated that the basic information risk management can stop up to 80% of the cyber-attacks seen today, allowing companies to concentrate on managing the impact of the other 20%. We recommend that as a business you take steps to review, and invest where necessary, to improve security in the following key areas:

Home & Mobile
Working Develop a mobile working policy & train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit & at rest.

User Education & Awareness
Produce user security policies covering acceptable & secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Incident Management
Establish an incident response & disaster recovery capability. Produce & test incident management plans. Provide training to the incident management team. Report criminal incidents to law enforcement.

Information Risk Management Regime
Establish an effective governance structure and determine your risk appetite - just like you would for any other risk. Maintain the Board's engagement with the cyber risk. Produce supporting information risk management policies.

Managing User
Privileges Establish account management processes & limit the number of privileged accounts. Limit user privileges & monitor user activity. Control access to activity & audit logs.

Removable Media
Controls Produce a policy to control all access to removable media. Limit media types & use. Scan all media for malware before importing on to corporate system.

Monitoring
Establish a monitoring strategy & produce supporting policies. Continuously monitor all ICT systems & networks. Analyse logs for unusual activity that could indicate an attack.

Secure Configuration
Apply security patches & ensure that the secure configuration of all ICT systems is maintained. Create a system inventory & define a baseline build for all ICT devices.

Malware Protection
Produce relevant policy & establish anti-malware defences that are applicable & relevant to all business areas. Scan for malware across the organisation.

Network Security
Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access & malicious content. Monitor & test security controls.

Source: The Information Security Arm of GCHQ (2012)

Conclusion

Computer and Information security in this generation is a vast topic that is fast becoming more important because the world is becoming more highly interconnected, with networks being used to carry out almost all critical transactions.

Cybercrime continues to diverge down different paths with each period that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organisations with not only how they secure their infrastructure, but how they require new architecture, platforms, and intelligence to do so. There is no perfect solution for cybercrimes, but concerted effort should be geared towards best to minimise them in order to have a safe and secure future in cyber space now and beyond.

References

Seemma, P., Nandhini, S., Sowmiya, M., (2018) Overview of Cyber Security International Journal of Advanced Research in Computer and Communication Engineering Vol. 7, Issue 11

Cyber security for Beginners www.heimdalsecurity.com

ACS Cybersecurity Threats Challenges Opportunities (2016)

10 Steps to Cyber Security CESG The Information Security Arm of GCHQ - GCHQ, BIS and CPNI (2012)

Perspectives on transforming cybersecurity Digital McKinsey and Global Risk Practice McKinsey & Company (2019)

Introduction to Cybersecurity: The introductory course for those who want to explore the world of cybersecurity: www.netacad.com

Mohamed, A., and Geir M., (2015) Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks Journal of Cyber Security, Vol. 4, 65–88

Kalakuntla, R., Vanamala, A; Kolipyaka, R., (2019) Cyber Security Associata Holistic Research Academic Holistica Vol 10, Issue 2, pp. 115-128

Personality Column with

MR TOPE SMART

Immediate Past President of AIO and
Group Managing Director
NEM Insurance Plc.

It is a known fact that many insurance operators today were initially birds of passage, as they came to the insurance industry, not by choice, but by accident. For Mr. Tope Samuel Smart, the case was different. He was quite deliberate after secondary school, even when many of his ilks were at sea about their future career. Young Tope settled to study Insurance at the University of Lagos and came out tops. Since there is no obstacle in the way of a determined mind that would be insurmountable, Mr. Smart rose meteorically through the ranks in the Nigerian Insurance Industry, becoming a Managing Director for greater portion of his career life. His impacts and contributions to the Insurance Industry, both locally and internationally, earned him the coveted position of the President of the African Insurance Organisation (AIO), which he held admirably for one year. Little wonder his peers gave him the sobriquet "Continental President". Mr. Tope Smart is a gift to the Nigerian Insurance Industry.

In this interview with the duo of Tope Adaramola and Helen Chiamaka Ajeamo, this iconic practitioner bares his mind on diverse industry issues and gave deep motivation to the younger generations. It is an interesting read.

What are your thoughts about the Chartered Insurance Institute of Nigeria (CIIN) and the Insurance Industry at large?

First and foremost, I want to appreciate the Editorial Committee of the Institute, I consider it a great honour to be interviewed for this column. The CIIN is the umbrella body of all insurance professionals in Nigeria, saddled with the responsibility of equipping its members with International best standards trainings on skillsets and professionalism. The Institute from time-to-time rolls out the codes of conduct that guides the professionalism and ethical standards of its members in the industry.

The CIIN equally collaborates with other relevant bodies both within and outside Nigeria; I am aware of its collaboration with the Chartered Insurance Institute, London (CII), as regards development on insurance practice. The Institute also partners with other bodies to organize programmes for the essence of keeping members abreast of trends in the industry. I am so proud of the Institute for the many innovations over the years, I believe the future of our dear Institute is brighter.

On the level of growth of the insurance industry, the industry has greatly evolved, I can boldly say we are not where we used to be though, we are yet to be where we ought to be. Notwithstanding, I am confident that very soon, we will be there, the industry is making a huge progress and am happy to be part of the process and advancement happening in the industry.

What were those peculiarities about the insurance industry yesteryears that we have lost now and how do you think we could recover them?

Well, there were some bad and some good habits. One major bad one was the inability of some companies to pay claims, such companies only collected premiums from clients but do not pay claims. This really dented the image of the industry. I recall someone told me then when he had a claim and proceeded to the insurance company to see the Managing Director after several mails were sent with no response from the company, he said after he expressed himself to the MD his response was "how much is your premium that you want claims"? This means they collected the premium without having any intension to pay claims. This negatively affected the industry then and is still hampering its growth. Also, poor regulation in the industry was another challenge. The regulators were not properly equipped to perform it roles of setting standards for the industry as at then.

On the good sides, we had a high standard of professionalism exhibited in the industry in the past by practitioners. We had very sound underwriting then that when you stepped into some companies you will marvel at the level of practitioners understanding of the ethics of the profession. They performed their duties with much diligence and expertise. There was proper underwriting process, rating, risk management mechanism and lots more were in place. Unfortunately, today that vacuum has not been so filled to an acceptable level, you rarely come across any kind of genuine commitment to underwriting today. Most practitioners are not interested in underwriting because they are concerned with getting premiums without weighing the risks; this is quite appalling. This is why today; many companies are not able to honour their claims obligations because they did not do proper underwriting. We have lost touch with this and I think it is a major area we need to address urgently.

Another good thing about the industry in the past was that we had markets leaders and specialized insurance companies. We had companies that were specialists in the various types of insurance policies and could direct clients to meet them to purchase policies. Those companies were at their best in their various product line unlike today where everybody does everything not considering if the company has the required expertise to carry out such operation.

Today, we practice Jack of all trade but I remember those days when we give specific businesses to specific companies for their peculiarities. This specialisation in the insurance business made them market leaders. In the good old days, these various market leaders were playing leading roles in all aspects of the market. I remember vividly if you take a particular business to a company and the company does not have knowledge and expertise about the business, such company directs you to a specialist in the business. The likes of Lion of Africa, Phoenix, Royal Exchange, Law Union and Rock Insurance Plc etc, were all identified as market leaders in their respected areas of business and you see other insurance companies follow their paths. We believed and trusted their inputs because they were regarded as market leaders with their various product lines.

Despite all these, we have so many positive values in the industry today, the industry is well capitalised unlike the yesteryears. We are also more dynamic and currently have a shift of focus compared to the old days. Technologically, the industry has greatly progressed vis-a-vis the past. Digitalisation is a great plus to the advancement of the industry.

How was experience as the past President of African Insurance Organisation (AIO)?

First of all, I like to thank God for the grace and privilege given to me to assume leadership position at AIO at that critical period. When I was going in as the President, I knew I was not only representing myself but Nigeria as a whole. So, I assumed the office with a prepared agenda. The agenda were:

- To achieve a successful tenure
- To perform beyond expectations
- To leave a lasting legacy

To the glory of God, I'm happy and proud to say I was able to accomplish the set goals to a reasonable point of assessment with several testimonies across board. I got a lot of feedback about my performance from members and I can say it was a successful tenure. I like to quote feedback I got from a member he said, "I have been in this AIO space for over 50 years, you are the best President I have ever seen" many other remarks along this line.

What I did was to change the narrative at the AIO. When I assumed office, I met and discussed with some Past Presidents and all I was told was "you do not need to have any agenda, the AIO is run by the Secretariat, so just follow the course" I objected to this because I was of a different opinion, I knew it was going to be the beginning of a new epoch and I told myself, whatever is worth doing, is worth doing well. I do not go for titles, what matters to me is the impact I made anywhere I find myself. Afterwards, I had a meeting with the Secretariat and I made them understand that I was aware of the practice and tradition but I want to be distinct. The Secretariat was so excited and gave a welcome gesture to my stand. They made me know they had been waiting for such an administration that will change the narratives. I rolled out my agenda to them, they bought into it and they gave maximum support required.

During my tenure, I visited several markets and this has never been done before. I bought AIO to the different markets but prior to this, AIO was perceived majorly as a ceremonial organisation which only appears when there are events. We visited several markets across Africa and honestly speaking, it was very impactful and the AIO became more visible business wise. People were very happy and excited that AIO came to visit their markets. During these visitations, we met Presidents, Governors, Ministers and other top government officials and we preached the importance of insurance to them. To my surprise many of them claimed not to have heard about insurance before and they were just hearing about AIO. This initiative was one of the major reasons why we recorded a massive turnout of delegates at the recently concluded AIO conference held in Kenya. We had over 2,000 delegates in attendance and this was the first time.

My goal for the visitations was to increase insurance penetration in the continent. Africa is behind when it comes to insurance adoption. In fact, my last days in the office were emotional for me as I had a plethora of positive feedback from all nooks and crannies of Africa as regards my impactful leadership. Aside the standing ovations I received, many testimonies noted that my Presidency offered much impact in such a short while and it may be difficult to find another President like me. In fact, such was the excitement of the people that the Secretariat asked me to extend my tenure and continue with such laudable development but I had to decline and assured them of unrelenting support whenever they needed it.

Challenges or regrets as the President of AIO?

Well, my tenure was quite eventful and impactful, I enjoyed my duty call, the only challenge I encountered was time constraint, there were lots of projects to execute but within a limited time frame. I wish I was able to visit more markets and countries to propagate the gospel of insurance.

Share your thoughts on the insurance industry public perception. Do you see the industry image in a better shape in the nearest future with the present approach?

Indeed, this has been one of the major problems we have in the industry and I must say we really have a lot to do. Yes, we have embarked on more publicity and image laundering to improve our public perception. However, I believe that so long as we have weak companies that are unable to meet their obligations, no amount of money spent on publicity can alter the negative public perception of the industry. For instance, if 99% of insurance companies are meeting their obligations but the remaining 1% is unable. The victim of this 1% can go any length to escalate his experience via various social media platforms, spoil the achievement of the larger percentage and this will mar the image of the industry. We must address the issue of weak companies in the industry.

So, companies need to meet their obligations promptly. When this happens, it is not only the industry that will be promoting insurance, the satisfied customers will also join in the promotion. It is their testimonies and experiences that will preach the insurance gospel.

Education is another feat for the industry. We need to educate and sensitize the masses about insurance, make them believe that the narrative has changed. Some people had horrible experiences in the past and vowed never to be involved in insurance, these set of people need to be re-oriented and have their mindset changed about insurance. We need to let them understand we pay claims, we need to do this with facts and figures in order to convince them.

The companies today are very responsive to claims payment, I can tell you authoritatively that NEM Insurance paid over N11 billion claims last year and many more companies of like minds. There are testimonies but the masses are not informed, they only hear the negative side of the story, so we need to intensify our publicity and education efforts. I believe that when all these measures are taken into consideration, negative publicity will be a thing of the past for the industry.

To what extent has the industry been able to bring the Government to play their role in the insurance sector?

It is quite unfortunate that the industry is not getting the support of the government as expected. With the government being the biggest spender in any given economy, insurance inclusion in government policies will greatly aid the propagation of insurance. So, we really need them to buy into insurance. The insurance industry lost a very huge opportunity during the administration of former President Goodluck Jonathan, the then Minister of Finance, Dr. (Mrs.) Okonjo Iweala organised a financial stakeholder meeting and was ready to give insurance a push for the first time. She expressed her interest in the industry and deliberated with us throughout the duration of the programme and set up about five committees need to transform the industry.

I was privileged to chair one of the committees which reported directly to her. We were making progress but sadly, this came at the twilight of that administration. The activities of the committees were abandoned at the emergence of a new administration. If that opportunity pulled through, it would have been the best for the industry.

How compliant is the industry when it comes to digitalization?

Well from my study, the insurance industry across Africa is slow in embracing technology. Taking the Covid-19 Pandemic as an instance, of all negative things attributed to the pandemic, the only good side of it is digitalisation. The pandemic triggered the industry to embrace digitalisation especially, during the lockdown as essential duties continued online, meetings and conferences were held virtually and lots more. Though the adoption level is slow but I believe that having started; it is a work in progress and insurance operators across Africa will soon come to fully embrace digitalisation in all their business operations to boost the insurance penetration rate.

What is your success secret in the industry?

First, I acknowledge the grace of God in my life, he has brought me this far, provided me all required assets to be where I am today. Also, I did not join the industry by accident. This is not to offend some of my colleagues but I know quite a number of my colleagues who got here by accident, most of them studied Economics, Accounting, Business Administration, Political Science and the likes. I enrolled to study insurance at the University of Lagos. I knew I was coming to the industry and I fully prepared for it. I got my motivation from my then Head of Department who doubles as my Lecturer. He is of blessed memory now. While teaching as an insurance Lecturer he never believed in insurance operation in Nigeria. He would mostly refer to the multinational insurance companies of those days and tagged indigenous insurance companies as broad street insurance companies. He believed core insurance was not practiced in Nigeria. This belief of his, challenged me to make a solemn vow that I will change the narrative of insurance practice in Nigeria. It was disheartening for me to know that our own Lecturer do not believe in us. I wish he was alive to witness the Nigerian insurance industry of today and the commissioning ceremony of the new NEM insurance house.

Another secret is my integrity; you will agree with me that integrity has become a scarce commodity in the world today. I value and keep to my words. Hard work is another value that has gotten me this far in life. I do not believe in cutting corners, I strongly believe in hard work. I always tell my children; both biological and foster children never to cut corners to

succeed. I charge them to work for success, hard work pays, success is never by accident, you have to make it work.

Discipline is also my super power, one must be disciplined and focused in life to achieve dream goals. I always tell the young ones, especially members of staff in NEM Insurance to always remain focused, disciplined and dedicated to their commitments, never get distracted by what others are doing, move at their own pace, be steady and with time they will arrive at their dream destination. I preach these values to them always because I strongly believe in them. I also remind them not to underestimate, disappoint and betray the trust of others. When you are trustworthy, more will be entrusted to you.

Word of advice to the young generation and what do you think the future holds for the industry?

My message to the younger generation is that they should believe and have a sense of commitment, purpose and stake in the insurance industry. There are potentials in the industry. The industry leads other financial bodies in the developed world and we need it to be at that level in Nigeria too. Though, there is a lot of brain drain at the moment due to the 'Japa' syndrome and it's affecting every sector of the nation but there is hope for us. I encourage young ones to see beyond the moment and view the potentials in the industry; it is largely untapped. To continually advocate this, four years ago I started the Graduate Trainee programme at NEM and it has been helping in terms of sensitisation for the young ones here.

Insurance is one of the few disciplines you can earn multiple incomes aside your salary, so it is a very lucrative profession. I had a friend's son who decided to join the industry after serving at NEM as an intern. This was because of his experience here. This is someone his father has been persuading to take up insurance as a profession but he refused until he had an experience working here. We need an enabling and conducive environment for insurance to thrive, and I believe when government buys into insurance, we will surpass all other sectors. If we are performing this well without the required government support, I am so certain that we will do better if government embrace compulsory insurances and the industry gets huge premium. The future of insurance is really bright and I believe it will bloom beyond our imaginations.

The Pivotal Role of CYBER SECURITY in the Insurance Industry

By Vera Aimufua

Introduction
The advent of the Internet of Things (IoT) which grew out of ARPANET (that foreruns the first network to use the Internet protocol) has advanced communication with distant – relationships in real-time, enhancing the operations of businesses including the insurance industry. Aimufua (2019) asserted that the risk of globalisation with advancement in information and communication technology (ICT) has engendered the paradigm shift in businesses and communication technology which has resulted in the continuous innovation in the contemporary application of computers software, hardware, networking, and other such critical communication systems. Also, the issues of storage, retrieval, transmission, or manipulation of data or securing information coupled with the infrastructures keep evolving.

In the recent past, a trajectory of growth in the ICT sector has caused every industry and human endeavor to adopt ICT at an increasing scale and sophistication. This is to support production and service delivery without the barriers of time and location while cutting down dramatically the cost of doing so. Interestingly, the storage of massive data in the insurance companies, which form major assets of the organisations might become the target of attacks as they adopt and decide to be a player in cyberspace. Aimufua and Dzidonu (2016) opined that the adoption of technology happens to be the vehicle that drives individuals or organisations to participate in cyberspace. Furthermore, the authors argued that technology adoption has been the driver of economic growth. While the technology infrastructures needed to operate in cyberspace are not wholly under the control of the organization. Thus, exposing the company assets to any form of attacks like intrusion attempts and financial breaches to organized state-sponsored attacks. In essence, insurance companies being players in the financial sector of the economy, it behooves them to adopt the ICT technologies, failure might cause a non-adopter to be dead in the water. In accepting to be players in cyberspace, the security of their tangible and non-tangible assets becomes imperative. In doing so, Shafqat and Masood (2016) suggested an urgent need to appoint an official body to lead the cybersecurity tasks at both national and sector levels. In order to think of security about various systems like installations, objects, appliances, and services, providing only physical security may not be enough. Hence, cybersecurity security should be considered as an equivalent target.

Cybersecurity Explained

The interconnectivity, automation of industrial processes, massive data collections and other phenomena that brought technologies have changed modern enterprises functionalities as well as indirectly societies and states economies. As such the physical world reality has entwined into the digital world. While the challenges and threats found in the physical world are daily creeping into the digital world as more advances are made. In short, technological advancement is impacting greatly on many spheres of human endeavor including security. In order to secure our properties with full auditing of the installations, software, hardware, appliances and services might only provide physical security which may not be enough (Shafqat and Masood, 2016). Thus, the need to also provide security for our cyberspace and corresponding infrastructures. In essence, cybersecurity is the measures taken in the protection of national and industrial infrastructures in the interconnected world against the cyber criminals or unauthorized access/use and ensures the practice of confidentiality, integrity and availability of information. Cybersecurity has actively been protecting programs, databases, systems and networks from unauthorized access, attacks, changes or destructions. Interestingly, as the insurance industry is met to understand and manage risk in the society, which in turn impact the society positively, understanding the concept of cybersecurity becomes essential.

Types of Cybersecurity Concept

The role of insurance industry is to understand and manage risks in the society, which could be enable her to impact on the society. The risk factors addressed in the real world are more less known with minor shade of unknown. However, in the digital world, the risk factors are high and mostly unknown by the practitioners. Once they are unknown, it might be difficult to safeguard them. Therefore, it is pertinent to identify some of the cyber threats and possibly proffer ways of safeguard them. It was reported in Cisco Annual cybersecurity report that the number of cyber-attacks has increased astronomically. While hackers are taking malware to an unmatched level of sophistication and impact. It behooves on the insurance practitioners to equip themselves with all knowledge available in order for the hackers not to get one off-guard. As knowledge of cyber threats may help in safeguarding organizations assets from cyber-attacks that could lead to both physical and financial loss. Some of the known cyber threats are:

- Distributed Denial-of-Service (DDOS) Attack: this is the art of flooding a network with more traffic than it can handle, which might cause the website to crash. In this case, the attack are launched from multiple devices aimed at a specific target.
- SQL Injection: is the art of injecting arbitrary SQL code into a web application database query with the intent of manipulating the backend database. The intent of this attack is for the attacker to extract or include private information there were initially not visible.
- Malware attack: these are different types of malicious software that are designed to breach the operation of your system including ransomware, spyware, viruses, and worms. It has the capability of being installed in a system and block access to important network components.

- Phishing attack: involves the use of fraudulent email to obtain sensitive information like personal information, bank details as it is deem to be from a trusted and reliable source.

Cybersecurity in the Insurance Industry

The insurance industry as a subsector of the financial services sector has in recent times adopted digital technologies to meet the increasing demand of her customers for services 24/7/365. This is besides the competition introduced by new digitally based business models that attempts to out-compete the traditional insurance industry. However, driving the insurance business with digital infrastructure has introduced new challenges arising from the cyber risk inherent in these technologies. The constantly evolving nature of the ICT industry further compounds the risk as new technology introduces new kinds of vulnerabilities that threat actors would exploit to the detriment of the entire industry, insurance companies, and policyholders.

Consequently, it has become urgently critical for the industry to ensure confidentiality, integrity, and availability of the information infrastructure, these goals define the crux of cybersecurity. In recent times, these goals have been extended to include the assurance that accountability or non-repudiation and authenticity are built into every information infrastructure

Cyber Value at Risk in the Insurance Industry

The insurance industry like every other financial service systems store Personally Identifiable Information (PII) of individuals and organizations in great detail. This may include, names, photographs, biometrics, credit card information, etc of customers. The compromise of any of this information poses a monumental risk to both the industry and the individuals whose data have been compromised. Thus, myriads of threats against the insurance industry, targeting these PIIs range from ransomware attacks, state-sponsored threats against the detailed PII resources, hacktivism that targets the industry for ideological reasons, etc.

In an instance of successful cyberattacks, the industry suffers in a variety of ways; namely; litigations, and lost trust from clients. On the side of policyholders, there will be cascaded impacts from the data stolen such as credit card frauds, social engineering, etc. All these combined wills threaten the industry's profitability and by extension survivability.

Treating the Insurance Cyber Risk

Generally, in treating cyber risk, organisations must look to existing cyber risk management frameworks like NIST, etc. However, the insurance industry must of necessity rebuild these frameworks along three key elements, viz: pre-attack (prevention), during the attack (response), and post-attack (recovery). The essence is to ensure that the industry develops preventative strategies to drastically reduce the rate of occurrence of successful cybersecurity events. However, systems cannot be fully-proof against cyberattacks, thus the industry must have a strong response and recovery strategy in place.

Additionally, the industry must architect her cybersecurity solution around the people, process, and technology framework (PPT framework). This will help the industry address the risk inherent in employees and other stakeholders (people), processes (policies, standards, and procedures) and technology. This comprehensive view will enable a holistic treatment of the industry's cyber risk.

Conclusion

Insurance companies are known to store large amounts of information about their policyholders. This practice makes them a target for cybercriminals.

The insurance sector is under pressure to embrace innovation and modernize its systems and infrastructure like the rest of the financial services industry its consumers demand services 24/7/365. Providing real-time insurance and financial services with a seamless and frictionless customer experience requires the latest infrastructure technology and this leaves this sector vulnerable to cyberattack. Insurance institutions should put machinery in place to build cyber resilient businesses that will not only protect themselves in the cyberspace, but also swiftly recover and resume business operations when attacked.
Insurance companies must get a grip of practical realities of data privacy through solutions offered by cyber experts with a focus to secure client information technology and network from cyber-attack threats.
Insurance institutions must engage cyber security experts who will provide a strong defence and good service skill in cloud technology and cloud securities as well as present an effective information security and expertise approach to their data protection.

References

Aimufua, G.I.O., and Dzidonu, C. K. (2016). Towards a general framework for analyzing technology acceptance – Adoption factors, Int. J. of Business Innovation and Technology (IJBIT), 3 (2), pp 1–8.
Kulugh, V.E., Okpala, E., and Aimufua, G.I.O. (n.d). Conceptual Design of E-Government Dependency Maturity Assessment Model,
Shafqat, N., and Masood, A. (2016). Comparative Analysis of Various National Cybersecurity Strategies, International Journal of Computer Science and Information Security (IJCSIS), 14 (1),
https://cybersecurityguide.org/industries/insurance

CYBER SECURITY and Insurance Solutions

By Osanaiye Olutoyin Adegoke
Manager, Great Nigeria Insurance Plc

Introduction

Many industries, including insurance, are adopting IoT technologies to evolve within this increasingly competitive market. One of the first entrants was Motor, closely followed by Home and Health. Each business line has an extended value proposition, for example, for Connected Car, the aim would be to manage its existing customer base and increase profitability. For Health it would be to grow in new customer markets, reward for good behaviour as well as adopt 'open' technologies such as platforms and devices.

Across all areas, common digital levers become apparent – to reshape claims management, enhance processes and efficiency, minimise fraud and to increase revenue through competition all achievable by harnessing the potential of data to add value.

Given the severe consequences of a security breach, it is critical to build on reliable and proven cryptographic cybersecurity solutions within the insurance sector.

Solutions for the Insurance Sector

Digital Transformation
Customers now expect to communicate primarily through mobile channels and experience faster and personalised offerings which combine both human and technological capabilities. This is being met by intertwining technology, processes, and people. After decades of working with paper-based documents and processes, the customer now can

use high-trust, secure and legally valid electronic signing solutions.
Digital transformation within the Insurance sector increases opportunity to win customers, improve performance, enhance customer loyalty and experience and to succeed long term (omeron.com, 2022).

In a data-hungry environment, insurers need to remain one step ahead recognising that emerging technologies such as IoT, advanced analytics, AI and Big Data will be crucial to driving new offerings such as:

- Predictive analytics- efficient tracking, trends and personalized products.
- Process automation for core business operations.
- Synchronous processes increase sales, productivity, and profits.
- Customer 'self-service' for products and services.
- Integrated design and systems enhance customer experience.
- Reduced cost and time in business operations.
- Improved claims processes and increased underwriting efficiency.

As innovative, disruptive, technology-led insurtechs are introduced within the insurance sector, this creates a competitive threat to incumbents, they also come with valuable opportunities to collaborate and meet on common ground: Data and the Customer.

Data Security & Compliance

As insurers develop a more digital experience, enhanced security design controls need to be considered, including authentication. Various regulations such as GDPR (EU Law), CCPA and CPRA (California Law) increase the rights of individuals and the responsibilities of companies handling personal data. Insurers need to see this as an opportunity to demonstrate trustworthiness to their customers.

The insurance sector generates large volumes of data that comes from a myriad of sources (policy records, claims, social media, credit reference agencies, sensors) with a requirement to be processed and analysed to ensure accuracy in terms of assess and price risk. Exploiting this data has unlimited advantages- fraud reduction, tailored policies, and improved customer segmentation (eiopa, 2022).

In line with consumers expectations towards all things digital, as well as various ways in which data is being collected, stored, processed, and analysed, cyber risk contributes to vulnerability as more and more data is accumulated.

In a highly regulated market, insurers would need to provide a comprehensive data governance solution with appropriate controls to ensure that relevant processing meets existing and evolving data privacy regulations.

Cryptography plays a major role in the implementation of secure systems: confidentiality, integrity, and authentication.

Big Data Analytics and Privacy in the Hybrid Cloud

Predictive analytics will expose trends of behaviour and common demographics and characteristics, resulting in revised and targeted marketing strategies, service delivery and distribution models, product range, risk selection and pricing structures. The hybrid cloud allows the data and the related analytical workload to be positioned where it makes the most sense in terms of business requirements. The information privacy and security are managed and controlled consistently across all the systems of the hybrid cloud environments (ncsc.gov.uk, 2022).

At the heart of digital transformation, data is king. And by not embracing big data, insurers can lose market strength and may face extinction.

In a dynamic and highly regulated industry, there are regulatory, compliance, security, and data protection requirements to consider. Cloud technology can enhance security by working collaboratively and effectively across functions whilst safeguarding the integrity, confidentiality, availability, and control of data through:

- Innovation: Unlock data in the cloud, information sharing for enhanced strategy.

- Improve speed to market: IT agility and shorter project implementation time.
- Business growth: New customer-oriented business models and potential for global expansion.
- Risk management: Integrate risk data and assessments within one environment.
- Cost reduction: Operating and capital investment costs are reduced.

A hybrid cloud gives reliability, performance, and flexibility to deploy different workloads on-premises and in the cloud to best meet the needs of customers now and in the future (globaliqx.com, 2022).

Secure and Technically Trustworthy InsurTechs

The transition from reactive to proactive business models, made possible by technology and data, is driving the rise of InsurTechs. However, InsurTechs have access to data that is more detailed and personalised, which raises data security and privacy concerns. Securely integrated service networks with ecosystems allow management on and off-premise helping insurers balance innovation alongside security requirements (techtarget.com, 2022).

InsurTechs are driving innovation and traditional insurers need to evolve.

No one likes buying insurance and therefore, attractive, simple, no-fuss products are key to the consumer. Sleek experience, easy turnaround, fast payout, no paperwork, no fuss.

In an industry that has been stable for many years, the insurance sector, vastly becoming digitally dependent, is now embracing the benefits that these insurgents can bring.

- In **commercial** insurance, the focus is mainly on enabling or extending the insurance value chain and therefore InsurTechs are viewed as potential partners.
- In **personal lines** insurance, this business model is under attack from a variety of cheaper, more agile digital InsurTech challengers where business is likely to take place as an online, mobile experience.

As InsurTechs enter this sector and see data analytics as their secret weapon to fuel their own business models; there is a common requirement across this industry, a necessity for the security of customer data whilst at rest, in motion or in use.

Conclusion

Insurance company does not only need to manage cyber and IT risk within the company and the value chain, they also need to keep pace with new threats and developments. It is important to implement appropriate requirement for cybersecurity solution in order to prevent cyberattack which can result in financial loss, data breach and insecurity within the insurance company. Insurance companies must be alert and dynamic when it comes to following the latest security technology. Thus, cyber-threats can be easily noticed and quickly eliminated to prevent potential financial and intangible harm.

References

https://omreon.com/cyber-security-priority-for-the-insurance-industry/

https://www.eiopa.europa.eu/media/feature-article/cyber-risks-what-impact-insurance-industry_en

https://www.techtarget.com/searchsecurity/definition/cybersecurity-insurance-cybersecurity-liability-insurance

https://www.ncsc.gov.uk/guidance/cyber-insurance-guidance

https://www.globaliqx.com/four-ways-insurance-improve-cybersecurity/

CYBER-SECURITY

A DISRUPTION OR INNOVATION IN THE INSURANCE INDUSTRY?

By **Obinna Chilekezi**, FCIB, FIIN, FPAM, FWAII
& **Margaret Jinadu**, B.Sc (ins), M.Sc. (Mgt), M.Sc (ins)

Abstract

It is no longer news that we live in a global village, a village of interconnectivity whereby one end of the globe is connected to another. The globalisation of the world which is a welcomed development, has also introduced changes in the taxonomy of risks. Risk is no longer risk as we knew them years back following the introduction of new risks, destruction of some old risks and the mutation of risks especially, in the area of information and technology. This paper adopted a qualitative research approach using secondary sources for review to determine the necessity of cybersecurity to the Nigerian insurance industry. The findings from the review showed that there has been improvement in cybersecurity in Nigeria, which however, is not the case with cyber insurance. This is a challenge to the Nigerian insurance industry to not only sponsor empirical studies on cyber insurance but also to introduce to the market cyber insurance. This will go a long way in complementing the efforts of the country in providing adequate cybersecurity for its citizenry. However, there are strong reasons to believe that cyberscurity will create disruption in the future both in the business of clients of the industry and that of the industry too.

Introduction

It is no longer news that we live in a global village, a village of interconnectivity whereby one end of the globe is connected to another. The globalisation of the world which is a welcomed development, has also introduced changes in the taxonomy of risks. Risk is no longer risk as we knew it years back following the introduction of new risks, destruction of some old risks and the mutation of risks especially in the area of information and technology. More so, globalisation, anchored on information communication technology, has led to the birth of complex risks such as what is known today as cyber risks.

What do we mean by cyber risks? In a simpler manner, we can describe cyber risks as those modern day risks associated to the use of information technology tools, appliances and processes. Africa according to Sibe (2022) has more than 600 million total internet users. Sibe, further argued that this is more than the total number of internet users in North America, South America and the Middle East. He then added that the last two decades have witnessed increased technology adoption in Africa. While this has obviously increased the efficiency of Africa's workforce, it has also come with associated risks—one of which is the risk of cyberattacks (Sibe, 2022). The researcher went to frown at what he had described as global nature of this risk which is not exclusive to Africa.

Sibe went further to reveal that a recent Interpol report , had shown that about 90% of African businesses are operating without the necessary cybersecurity protocols and, therefore, are pruned to cyberattacks. The report also noted that there were more than 700 million threat detections in Africa within a one-year period. French newspaper Le Monde (via the Council on Foreign Relations) on the other hand had previously reported that the servers of the Chinese-built Africa Union headquarters in Ethiopia were bugged and that data had been routinely transmitted at night through a backdoor between 2012 and 2017. While China had denied this allegation, this is a classic example of how the continent is exposed—even at such high-level institutions (Sibe, 2022). This shows the hugeness of the lack of installation of adequate cyber security to organisations in the continent, of which Nigeria is not exemption to this, both governmental and non-governmental agencies.

Conceptual Review of Cybersecurity

Cyber according to Uwadia (2018) is the surfing of internet with a view of getting information, processing, retrieving, saving, upload, download and so on. On the other hand, there is an attempt here to adopt a simple meaning of cybersecurity for the purposes of this paper. Cybersecurity according to Rouse (2022) is a broad, umbrella term that describes any preventive measures designed to protect information from being stolen, compromised or attacked. Little wonder then that it could also be seen as a process using computer application to prevent, protect and control systems, networks and data from cyber attacks. This protective devise should be holistic in ensuring that compromise which could lead to cyber losses are prevented or forestalled.

Similarly, the Economic Times of India has referred to it as cyber security or information security, which it had described as the techniques of protecting computers, networks, programs and data from unauthorised access or attack that are for exploitation. In a more narrow position, Frankenfield (2022) observed that cybersecurity is a measure taken to protect inter-connected devices, networks, and data from unauthorised access and criminal use. Frankenfield added that it ensures the confidentiality, integrity, and availability of data over its entire life. In this way, this scholar had maintained that cybersecurity would apply to software and hardware, as well as information on the internet. Thus, it provides protection to systems, networks and data from personal information to complex government systems against malicious attack.

Cybersecurity Policy in Africa

We will attempt to review global ranking of cybersecurity and then narrow it down to Africa. The International Telecommunication Union (ITU), according to Oluwole (2022) has released the latest Global Cybersecurity Index (GCI) showing a growing commitment worldwide to tackle and reduce cybersecurity threats. This index took consideration of each country's development is assessed along the five strategic pillars of the Union's Global Cybersecurity Agenda (GCA): Legal Measures, Technical Measures, Organisational Measures, Capacity Building, and International Cooperation. This is then aggregated into an overall score. The current assessment covers the 2019-2020 period and reflects data collected during the Covid-19 pandemic. On the global scene, the ranking is presented as follows:

Country Name	Score	Rank
United States of America	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirate	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada	97.67	8
France	97.6	9
India	97.5	10

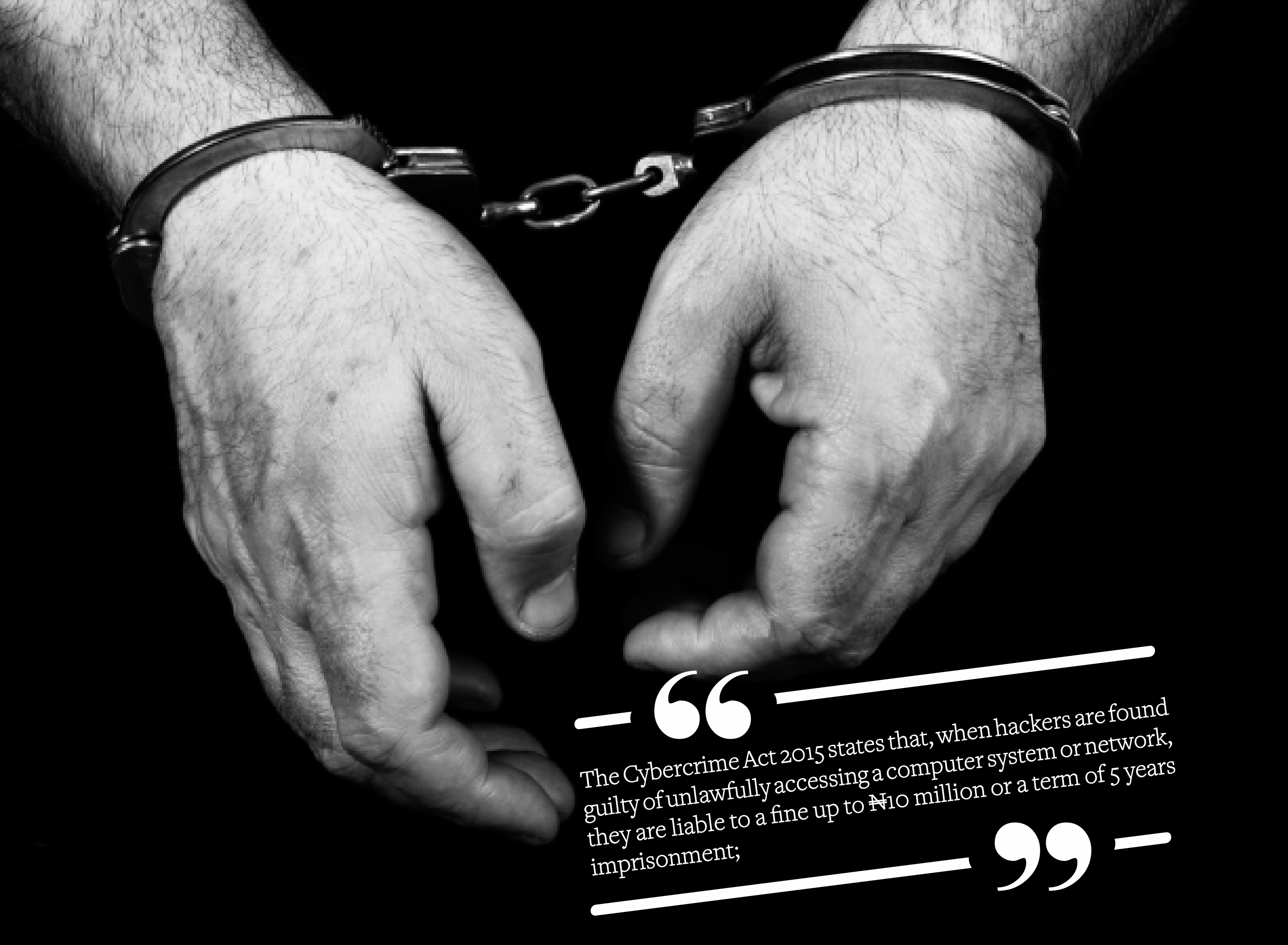
Source: International Telecommunication Union (2020)

On the African scene using same source, the African countries top ten are:

Country Name	Score	Rank
Mauritius	96.89	1
Tanzania	90.58	2
Ghana	86.69	3
Nigeria	84.74	4
Kenya	81.7	5
Benin	80.06	6
Rwanda	79.95	7
South Africa	78.46	8
Uganda	69.98	9
Zambia	68.88	10

International Telecommunication Union (2020)

It is pertinent to note here that the International Telecommunication Union (ITU) is the United Nations specialised agency for information and communication technologies (ICTs), driving innovation in ICTs together with 193 Member States and a membership of over 900 companies,



> The Cybercrime Act 2015 states that, when hackers are found guilty of unlawfully accessing a computer system or network, they are liable to a fine up to ₦10 million or a term of 5 years imprisonment;

universities, and international and regional organisations. It was established over 150 years ago (Oluwole, 2022). Having seen both the global and regional, it is pertinent to discuss the challenges of the Continent on cybersecurity.

On what African leaders should do on cybersecurity Kagama (2018) in address to the African Union had said that "Africa must take full advantage of the digital revolution to empower its citizens and enhance transparency in government and the private sector. This will not happen until data is stored in safe and trusted systems that protect privacy and are difficult for criminals to breach." This is an axiomatic position that cannot be faulted at all. Incidentally, most African countries are not showing much seriousness on issues of cybersecurity in their countries.

Cybersecurity in Nigeria

It is quite interesting that there have been a lot of empirical works on cybersecurity from our review for literatures on the subject. This is a welcomed development as it shows that Nigerians, as a people are taking the issue very seriously as it should be. Nevertheless, as revealed by Uwadia (2018) the issues pertaining to increase in cybersecurity in Nigeria could be linked to the following factors:

- Poor safety measure of handling laptop
- Assigning more than one password to people
- Use of flimsy/trivial or stress-free to predict password
- Not shutting down computer when not in use
- Negligence to firm or association security programs
- Social media

On the way forward, Uwadia cited the Cybercrime Act 2015 that supports prosecution as a way forward to curb cyber insecurity in Nigeria. He listed some of the provisions of the Act which could help in curbing the threats, such as:

(a) The Nigerian Cybercrime Act offers the President the power to assign computer system, networks, and information infrastructure relevant to national security of Nigeria or the economic or social well-being of its citizens as constituting Critical National Information Infrastructure;

(b) The Cybercrime Act 2015 states that, when hackers are found guilty of unlawfully accessing a computer system or network, they are liable to a fine up to ₦10 million or a term of 5 years imprisonment;

(c) Death penalty is advocated by the Nigerian Cybercrime Act 2015 for an offence committed in contrast to a system or network that has been labeled critical national infrastructure in Nigeria that results in the death of an individual;

(d) It makes provisions for identity theft, with the punishment of imprisonment for a term of not less than 3 years or a fine not less than N7 million;

(e) It states that creation of Child Pornography site is a crime punishable of imprisonment for a term of 10 years or a fine of not less than N20 million or both;

(f) The crime of crooks, cyber-stalking and cyber-bullying is punishable with imprisonment of not less than 10 years or fine of not less than N2 million or both;

(g) It prohibits cyber squatting, which registering or using an internet domain name with bad faith of making a profit, etc.

The passage of this Act may help the country to address the notoriety that it has acquired in cybercrime, especially financial scams, facilitated through the use of the internet (Makeri, 2017). Since the issue of cybersecurity is raising a number of questions in the minds of Nigerians (Makeri, 2017).

Cybersecurity and the Nigerian Insurance Industry

The Nigerian Insurance Industry is an industry which has embraced technology in virtually all of its operations and as such is prune to cyber risks and cyber attacks hence, the need for the industry to pay greater attention to issues bordering on cybersecurity on its operations and those of its alarming clienteles. It is pertinent to note that there have been little or not much empirical studies in this area by scholars. This then is a clarion call on the relevant authorities like the Chartered Insurance Institute of Nigeria, National Insurance Commission, etc to look at this direction in sponsoring such research activities on impacts of cyber risks on the Nigerian insurance industry.

It is not out of place also to note that the Nigerian insurance industry should develop both cyber liability insurance policies and cyber insurance policies to cater for the risk exposures on Nigerians in this area. As students of insurance and risk management, we do know that risk control should always have two facets of physical control (where cybersecurity comes in) and financial control (where insurance place its roles).

Conclusion

Cybersecurity is becoming prominent in Nigeria based on the findings from our literature reviews however cyber insurance is not in the country. This is a challenge to the Nigerian insurance industry to sponsor empirical studies on cybersecurity and also to introduce to the market cyber insurance. This will go a long way in complementing the efforts of the country in providing adequate cybersecurity of its citizens. There are strong reasons to believe that cybersecurity will create disruption in the future both in the business of clients of the industry and that of the industry too.

References

Frankenfield, J. (2022). What is Cybersecurity? Investopedia, retrieved online 08/09/22

Makeri, Y. A. (2017). Cyber Security Issues in Nigeria and Challenges. International Journal of

Advanced Research in Computer Science and Softwares Engineering, 7(4), 315-321

Oluwole, V. (2022). Top 10 African Countries with the best cybersecuirty. Business Insider, retrieved online 09/09/22

Rouse, M. (2022) What does cybersecurity mean? N.P. retrieved online 09/09/22

Sibe, R. (2022). Africa's Chaotic Legal and regulatory Cybersecurity Landscape requires

harmonization. Forbes, 1-2, retrieved online 07/09/22

The Economic Times of India (2022). What is Cyber Security, retrieved online 09/09/22

Uwadia, F. (2018). Cyber Security in Nigeria: Issues, Challenges and Way Forward.

International Research Journal of Advanced Engineering and Science, 3(2), 351-354

HOW CYBER SECURITY IMPACTS THE INSURANCE INDUSTRY

By Emmanuel Chilaka
IT Department, FBS Reinsurance

INTRODUCTION

The internet has made the world smaller in many ways, but it has also opened us up to influences that have never been so varied and so challenging. As fast as security grew, the hacking world grew faster. The range of operations of cyber security involves protecting information and systems from major cyber threats. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge. Insurers must commit to protecting sensitive customer information in a compliant and reliable way. The cybersecurity threat is huge. It is time for insurance companies to reboot their approaches to cybersecurity.

WHAT IS CYBER SECURITY?

In a computing context, security comprises of cyber security and physical security. Both are used by enterprises to safeguard against unauthorised access to data centre and other computerised systems. The security, which is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security. Cyber security therefore is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks.

HOW DOES CYBER SECURITY AFFECT INSURANCE?

With the advent of technology, improving day by day. Insurance companies are known to have adopted the storage of large amount of data about their policyholders. These activities make them prone to cyber-attacks if the necessary security solutions are not put in place. From projections, cyber-attacks on the insurance industry and other industries will continue to grow in rate and severity.

As the world embraces technology in most of its operations, the emergence of new cyber risks creates a highly complex situation, insurers not only look to cover the eventualities but also to prevent

such risks from materialising. Insurers should also provide post-event assistance to prevent further degradation or escalation of outcomes.

The Nigerian insurance sector especially, is under high gravity to employ innovation and modernise its systems and organisation. Providing real-time insurance and financial services with a seamless and frictionless customer experience that requires the latest infrastructure technology and highly skilled manpower.

With an increasing number of users, devices, and programs in modern insurance enterprise, combined with the increased deluge of data, much of which is sensitive or confidential, the importance of cybersecurity continues to grow. The growing volume and sophistication of cyber attackers and attack techniques compound the problem even further.
To this end, maintaining cybersecurity in a constantly evolving threat landscape is a challenge for all organisations. Traditional reactive approaches, in which resources were put toward protecting systems against the biggest known threats, while lesser-known threats were undefended, is no longer a sufficient tactic. To keep up with changing security risks, a more proactive and adaptive approach is necessary. The National Institute of Standards and Technology (NIST) recommends adopting continuous monitoring and real-time assessments as part of a risk assessment framework to defend against known and unknown threats.

Cybersecurity also needs to be infused into new software and applications with the latest technologies and patches to reinforce maximum and automated protection in real time.

WHY IS CYBERSECURITY IMPORTANT IN THE INSURANCE SECTOR?

Now that other high-profile sectors are becoming more secure, cybercriminals are turning their attention towards more vulnerable targets like insurance companies.

Insurers typically maintain a massive database of personally identifiable information about policyholders,

making them the perfect target for identity thieves. Information organisations keep about policyholders can include names, birthdates, social security numbers, home addresses, employment data, email addresses, payment information, and more.

Anthem Healthcare is infamous for holding the record for the biggest data breach in the history of the healthcare system. In 2015, Anthem Healthcare experienced the theft of 78.8 million records, including names, social security numbers, addresses, and birth dates. Hackers used spear-phishing to manipulate employees into handing over usernames and passwords, allowing them to access the insurer's systems. Not only did Anthem Healthcare experience massive data loss, the insurance company also experienced significant monetary damages. Recently, Anthem had to pay almost $40 million in damages, in addition to the $115 million to settle a class-action lawsuit.

With a huge database of information about policyholders, it is no doubt the insurance sector is a highly attractive target for hackers. Therefore, insurance companies must start adopting security measures that efficiently protect user information sooner, rather than later.

TIPS FOR BOOSTING CYBER SECURITY IN INSURANCE

Assess your defense capabilities realistically: Pressure-testing the insurance company's defenses can determine whether they can repel targeted, high-impact attacks, whether external or internal. It includes vulnerability assessment, testing programs, penetration tests, and scenario-based testing. Consider hiring a cyber-security firm to test your defenses.

Invest in early detection: Insurers need to continually invest and innovate to thwart potential attackers.

Early detection is crucial. Otherwise, a cyber-attack can sit undetected for weeks. Efficient and quick detection and response will help determine the source of the attack, the systems targeted, extent, and cause. Then, the threat can be neutralized before damage is done. Insurers need to invest in technology. There is a wide range of software solutions that provide real-time threat detection.

Making cybersecurity everyone's job: While implementing sophisticated systems will reduce external threats, insurers tend to neglect internal threats such as human error, which could include revealing customer data in response to a convincing phishing email.

Cybersecurity awareness among employees can significantly decrease the risk of cyber-attacks resulting from human error. Alert employees can provide early detection. An Accenture survey found that up to 98% of security breaches that are not detected by a firm's security team are discovered by employees.

Learn from the past and evolve: Effective cybersecurity requires insurers to learn from previous cyber incidents and use this to improve planning and technology investments. Solutions include:

- Upgrading systems: Using last-generation or unpatched security software provides easy fodder for cyber attackers. Speak to your IT consultant about upgrading your systems.
- Migrating systems to the cloud: The cloud provides users a wide range of compliant and secure storage solutions. Choose a cloud provider that offers the highest possible security.
- Implementing appropriate security software, protocols, and appliances: this will effectively shield data and systems from automated threats.
- Establishing a disaster recovery plan: Despite all efforts, systems can be breached. Have a detailed up-to-date plan so that you can respond effectively to any problem, major or minor.

Cyber-crooks are relentless and determined. Security is an ongoing battle. You can't afford to let down your guard for a seconds. Staying one step ahead of hackers takes constant effort.

CONCLUSION

The high levels of risk faced by the insurance industry, combined with the abundant resources of a lucrative business model, create an environment that attracts the best and the brightest in security solution research and development.

This sector offers many opportunities for security professionals at all levels. Trust is the very essence of insurance and is, therefore, crucial for the industry to thrive. Security professionals looking for a place to make a real difference in the lives of many people need to look no further than the insurance industry. The insurance industry must in turn invest in quality awareness/ trainings for employees and also provide adequate tools to mitigate cyber incursions.

REFERENCES

1. https://www.mindtree.com/insights/blog/cyber-security-growing-priority-insurance-industry
2. https://content.naic.org/cipr-topics/cybersecurity
3. https://www.globaliqx.com/four-ways-insurance-improve-cybersecurity/
4. https://www.researchgate.net
5. https://www.eiopa.europa.eu/media/feature-article/cyber-risks-what-impact-insurance-industry_en

> Artificial Intelligence, Machine Learning and Deep Learning: Artificial intelligence (AI) establishes the foundation for innovative technologies and processes to be deployed across the cybersecurity landscape, particularly in the automation of threat identification and detection. Furthermore, AI analyses large volumes of data breaches and network activity to speed up threat response and protect attack targets.

Cybersecurity:

A Disruptor or Innovation?

By Samuel Mbonu

According to the Oxford advance dictionary, Innovation is the introduction of new things, ideas, or ways of doing something whilst Disruption is the act of stopping something from continuing in the normal way.

With the dynamic and unpredicted traits of new technologies, its disruption is happening across industries, changing the landscape of business models and operations. From how we do business to how we socialise and travel to how we communicate, we depend on computer systems to drive these processes. With approximately 3.9 billion users, the internet has become one of the most significant technological developments. However, while widely accepted for its ease and efficiency, it is also embedded with many vulnerabilities, which pose substantial security threats to users and have resulted in increased cyber attacks.

As a result of our interconnectivity, there is a new need to adopt new, innovative technologies to protect organisational assets from evolving threats and attacks. To address these concerns, cybersecurity plays a significant role because its applications present initiatives for a secure environment, which in turn affect industry functionalities, resulting in a mental shift in which individuals and organisations must quickly adopt its capabilities. Failure to prioritise cybersecurity can be extremely detrimental to an economy, and it will almost certainly become a major issue for others as the economy digitalises. The prevalence of cyber security breaches have increased, and cybercrime is now one of the top concerns for CEOs worldwide. There is also a direct economic cost to businesses targeted by such attacks, such as theft of corporate information, disruption in normal operations, and even having to repair affected systems, all of which result in financial loss. Aside from the immediate consequences of a cyber-security breach, there are also legal ramifications including, regulatory infractions.

From the foregoing, the importance of cybersecurity for any forward-thinking organisations, especially financial service companies as they continue to adopt digital transformation technologies cannot be over emphasised. Innovation in cybersecurity are majorly driven by emerging and disruptive technologies. As this evolution continues, cybersecurity becomes more prominent. It can be said that cybersecurity seats nicely in the disruptive domain as well as the innovation domain.

Innovation in Cybersecurity led by Emerging Technologies

As our day-to-day activities rely heavily on technology, cybersecurity is mission critical to how businesses and organisations operate worldwide, even as evolving threats and attacks threaten the benefits of cybersecurity. This also strengthens its viewpoint as a technological disruption because it introduces new approaches for individuals, organisations, or both to protect organisational assets. Today, innovation within cybersecurity is significantly improving how technology can be used securely and enhancing the mode by which increasingly complex attacks are protected from causing damage to organisational assets. While cybersecurity represents an innovative approach in every sector of today's digital economy, innovative technologies enable organisations to implement and provide secure control mechanisms to businesses. This article will look at cybersecurity innovations that address the dynamism of threats and attacks while also adding value to organisations. They are:

1. Artificial Intelligence, Machine Learning and Deep Learning: Artificial intelligence (AI) establishes the foundation for innovative technologies and processes to be deployed across the cybersecurity landscape, particularly in the automation of threat identification and detection. Furthermore, AI analyses large volumes of data breaches and network activity to speed up threat response and protect attack targets. In cybersecurity, deep learning can detect threats, monitor network traffic, and analyse user behaviour in real time. On the other hand, machine learning can be used in cybersecurity for vulnerability discovery, automated breach investigations, and attack response. Innovative technologies like AI are constantly improving and providing valuable insights on how to offset sophisticated attack methods.

2. Blockchain: The adoption of Blockchain promises a new dimension of secure business transactions by ensuring data confidentiality (privacy), integrity, and availability. Its invulnerability structure of a distributed server with the properties of an impenetrable wall prevents cyberattacks and fraudulent network activities. In addition, blockchain technology allows you to set the required security levels for the system, protecting the entire system against falsification.

3. Zero Trust Model: The Zero-trust model is an innovative approach to cybersecurity that, unlike traditional security, enforces that no part of a computer and networking system, including the humans operating it, can be implicitly trusted. Instead, it requires all users to be authenticated and authorised before accessing data and resources, even if they are within the organisation's enterprise network. In addition, using a zero-trust model entails identifying critical data, mapping its flow, logical and physical segmentation, and constant endpoint monitoring, all of which assure that the systems and their components are operating appropriately, typically under a "least privilege" model, which is continuously verified.

4. Quantum Computing: Researchers all over the world are working to make quantum computing a reality, as it has the potential to disrupt cybersecurity and the technological landscape. For example, quantum computing opens up an infinite number of decryption options, potentially ending the current method of public-key encryption technologies. This is due to its ability to briefly factor large prime number equations, ranging from minutes to days. Unfortunately, this means that a quantum computer will soon be able to breach today's cybersecurity infrastructure. However, just as it provides a powerful force for attackers, industry experts will use quantum computing within cybersecurity to help detect and deter quantum-based attacks.

In summary, that rapidly evolving threat, combined with exponentially accelerating and converging technologies, presents a new cybersecurity paradigm, and innovation plays a critical role in this paradigm shift, as organisations must deploy new and innovative technologies, such as AI or even quantum computing. It is essential for cybersecurity professionals to consider innovative methods even as we begin to adopt disruptive technologies to ensure that security is integrated from the beginning to the end of any business process.

References

(2022). Retrieved 1 September 2022, from https://innovationcloud.com/blog/cybersecurity-innovation-as-the-backbone-of-digital-transformation.html#:~:text=Cybe rsecurity%20inno vation%20as%20the%20backbone%20of%20digital%20transformation.,and%20resources%2C%20even%20when%20they%20...%20More%20items.

(2022). Retrieved 1 September 2022, from https://www.irishtimes.com/special-reports/2022/08/25/innovations-in-cybersecurity-technology/.

7 Technology Innovations That Will Impact Cybersecurity in 2022 | CSA. Cloudsecurityalliance.org. (2022). Retrieved 1 September 2022, from https://cloudsecurityalliance.org/blog/2022/03/27/7-technology-innovations-that-will-impact-cybersecurity-in-2022-and-beyond/.

Cyber AI: Real defense. Deloitte Insights. (2022). Retrieved 1 September 2022, from https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html.

Cybersecurity Innovation – Transforming the Enterprise. Defence IQ. (2022). Retrieved 1 September 2022, from https://www.defenceiq.com/cyber-defence-and-security/articles/cybersecurity-innovation-transforming-the-enterprise.

Duc, H. (2022). Top 7 Cybersecurity Innovations in 2020. Pentestmag. Retrieved 1 September 2022, from https://pentestmag.com/top-7-cybersecurity-innovations-in-2020/.

Gillis, T., Unit, T., Holzworth, M., Staff, E., Worstell, K., & Worstell, K. et al. (2022). The Cybersecurity Innovation Mindset. VMware Security Blog. Retrieved 1 September 2022, from https://blogs.vmware.com/security/2022/03/the-cybersecurity-innovation-mindset.html.

Smith, T. (2022). Cybersecurity: Innovations to Look Out for in 2022 | The Fintech Times. The Fintech Times. Retrieved 1 September 2022, from https://thefintechtimes.com/cybersecurity-innovations-to-look-out-for-in-2022/.

The future of cyber security: 2022 predictions from Darktrace - Darktrace Blog. Darktrace.com. (2022). Retrieved 1 September 2022, from https://darktrace.com/blog/the-future-of-cyber-security-2022-predictions-from-darktrace.

The Future of Cyber Security: What We Can Expect. GradesFixer. (2022). Retrieved 1 September 2022, from https://gradesfixer.com/free-essay-examples/the-future-of-cyber-security/.

The Future of Cybersecurity. Security Intelligence. (2022). Retrieved 1 September 2022, from https://securityintelligence.com/the-future-of-cybersecurity/.

> Zero Trust Model: The Zero-trust model is an innovative approach to cybersecurity that, unlike traditional security, enforces that no part of a computer and networking system, including the humans operating it, can be implicitly trusted. Instead, it requires all users to be authenticated and authorised before accessing data and resources.

The Institute was founded in 1959 by Article of Association and Memorandum. The Institute was known and referred to as the Insurance Institute of Nigeria until February 26, 1993, when it became Chartered vide Decree (now Act) No 22 of the Federal Republic of Nigeria. Upon establishment in 1959, the Institute became the rallying point for insurance practitioners in Nigeria comprising a few Expatriates and their Nigerian counterparts whose pioneering effort provided the building blocks for what has now become a veritable force in the Nation's Financial Services Industry and the economy at large. The Institute was affiliated to the Chartered Insurance Institute (CII), London in 1960 for reasons bordering on the need to model its operations after the London Institute which then produced the bulk of insurance professionals whose expertise were indispensable in shaping the face of professionals' practice in the days.

www.greatnigeriaplc.com

gni

GREAT NIGERIA INSURANCE PLC
RC 2107

GNI COMPLEX, 8, OMO-OSAGIE STREET,
OFF AWOLOWO ROAD, IKOYI-LAGOS.
+ 234 - 1 - 3429161 + 234 814 247 88 29
info@greatnigeriaplc.com

MOTOR INSURANCE

Third party motor insurance
Starting from N5,000

Motorflex N7,500;
(Third party plus N100,000)
Own damage cover

Comprehensive insurance

FIREPROOF INSURANCE

N1000: 500,000 cover
N1,750: N1,000,000 cover
N4,000: N2,000,000 cover

GREAT SAVERS DELIGHT

An investment linked savings plan
Min of N100 per day
Min of N2,500 per month
Free minimum life cover
Guaranteed 5% interest rate
Minimum one year plan.

PERSONAL ACCIDENT INSURANCE

N1000: Death/Disability: N500,000
Public Liability: N100,000 Eye Glasses: N5,000

N1,900: Death/Disability: N1,000,000
Public Liability: N250,000 Eye Glasses: N5,000

N2,500: Death / Disability: N1,500,000
Public Liability: N400,000 Eye Glasses: N5,000

NAICOM/CA/ADV/2016/1545