ASSOCIATION OF KENYA INSURERS

INFORMATION PAPER ON CYBERSECUIRTY AND MITIGATION

ASSOCIATION OF KENYA INSURERS
P. O. Box 45388-00100, Nairobi
AKI Centre, Mimosa Rd, Mucai drive, Off Ngong Rd
Tel: 254 20 20273/330-3
Mobile: 0722 204149 | 0733 610325
Email: info@akinsure.com
Website: www.akinsure.or.ke

CYBER SECURITY AND MITIGATION

Introduction

Rapid technological developments have made it easier to use, create, manage and exchange information making life easier and better. Technology has provided vast areas of new opportunity and potential sources of efficiency for organizations of all sizes. Today's world is more interconnected than ever before, internet is rapidly becoming the most critical infrastructure for economies around the globe making us more reliant on technology. However, this increased connectivity brings unprecedented threats including increased risk of theft, fraud and abuse.

Cyber security is the protection of information systems from theft or damage to the hardware, software and the information on them as well as from disruption of the services they provide. Cyber security will continually become more important as more and more devices become connected to the internet.

Most of the companies have invested in technology to efficiently collect, process and store huge amounts of data. Big data is indeed the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. This makes cyber crime the greatest threat to every profession, every industry and every company in the world.

The volumes of attacks are increasing because to the attackers, the risks are low and the returns are great. The internet makes most attacks anonymous and untraceable because the attack is routed through hundreds or thousands of PCs in dozens of countries and that is really attractive to cybercriminals.

Cyber crime damages trade between nations, competitiveness, innovation, and global economic growth, and slows the pace of global innovation.

Global Overview

Cyber security is growing at a very fast rate. Global spending is estimated to be $77 billion (USD) in 2015; this is projected to increase to $170 billion (USD) by 2020.

The U.S. government has spent $100 billion on cyber security over the past decade, and has $14 billion budgeted for cyber security in 2016.

Cyber-attacks are costing businesses $400 to $500 billion a year, which includes direct damage plus post-attack disruption to the normal course of business; this does not include the large number of cyber-attacks that go unreported due to prospect of legal action against those that own up to cybercrime and the fear of damage to organization's reputation which can have negative impact on revenues, company valuation when raising capital, customer acquisition and retention, and their ability to recruit top talent. A significant portion of cybercrime goes undetected, particularly industrial espionage where access to confidential documents and data is difficult to spot.

It is projected that 2016 will see even greater numbers of cybercrime attacks on individuals, firms and government agencies as the 'Internet of Things' further develops, reliance on social media grows and a profound amount of personal information and data continues to be collected. Cyber attacks are estimated to cost the global economy up to $90 trillion by 2030 if cyber security fails to advance at a rapid pace.

Banking and financial services is the fastest growing non-government cyber security market, followed by IT and telecom, defense, and the oil and gas sector.

There is a global cyber security labor epidemic; the worldwide shortage of information security professionals is at 1 million openings, more than 200,000 U.S. cyber security jobs are unfilled. As cyber attacks and data breaches increase each year. The demand for the (cyber security) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million

The African region has also been facing increasingly sophisticated cyber-attacks fuelled by increasing internet penetration requiring adequate security measures. The Africa cyber security market is estimated to grow from $0.92 Billion in 2015 to $2.32 Billion by 2020.

Kenya

Increased internet penetration and technological advancements in Kenya have been driving innovation and business growth. Our Internet-based annual economic outputs are currently valued at approximately Kshs100 billion, but the same innovations are also exposing the public to cyber security threats.

According to the Kenya Cyber Security Report 2015, Kenya is losing about 15 billion shillings ($146 million) annually due to cybercrime up from 2 billion shillings ($22.56 million) in 2013. The public sector lost about Sh5 billion, followed by financial services sector at Sh4 billion. Manufacturing and industries lost Sh3 billion while telecommunications, media and technology and other sectors losses stood at Sh2 billion and Sh1 billion respectively.

70% of Kenyan businesses and nearly all internet devices are exposed to the risk of malicious insiders and cyber criminals as most network appliances are still configured with their factory default settings. Government websites and banking institutions remain the most vulnerable targets, most of their websites are developed externally but they rarely do a check on their security settings or update them.

In Kenya, malicious insiders are the main contributors to Cyber attack/ fraud, these are mainly employees assigned privileged access to systems, as they are aware of all the security devices and procedures in place, access systems and make unauthorized changes to key financial and consumer systems, transfer money illegally and steal customer/brokerage files. The latter attack is often more difficult to identify and recover from.

Investment in cyber security is still very low by most government agencies and other private businesses. The budgets allocated to implement security measures are inadequate and leave organizations open to various vulnerabilities

Kenya still faces a shortage of information security professionals considering that we have approximately 1000 certified ICT risk professionals compared to over 27 million internet users in the country.

Insurance Companies Cyber Security Vulnerability

Insurance companies are not exempt from cyber threats as they are becoming more reliant on technology. Insurers are innovating more by moving to digital, data-driven initiatives including collecting data from Internet enabled devices and enabling the mobile to undertake key processes like approving payments and funds transfer.

In 2015, major data breaches affected the insurance industry. In February 2015 Anthem, the second largest health insurance company in the United States, suffered a major data breach affecting 80 million current and former customers and employees where information that could facilitate identity theft was stolen including names, dates of birth, member ID/ social security numbers, addresses, phone numbers, email addresses and employment information

In March 2015, Premera Blue Cross, a major insurance provider in Alaska (the third largest health insurer in Washington State), also suffered a major data breach affecting 11 million people, the cyber attackers targeted sensitive personal information that could facilitate identity theft i.e. Member name, Date of birth, Social Security number, Member identification numbers, Email address, Mailing and/or physical address, Telephone numbers, Banking account numbers, Clinical information, Claims information. The attack began in May 2014 and was discovered eight months later on 29 January 2015.

All insurance companies are at risk for data breaches due to the great amount of clients' confidential information that they possess. Insurers must take measures to ensure their clients' information is secure and mitigate any potential risks.

Reducing the Risk

There are specific tangible measures that can help reduce the risk of data breaches. These measures include:

Government Intervention/Support: The Government should establish a systematic mechanism to track, collect, calculate and publish data on cyber crime losses to help companies and other countries make better choices about risk and policy.

Regulations and Compliance: Industry Regulators should carry regulatory compliance checks which require companies to implement relevant controls to mitigate risks; this will force companies to implement security controls.

Cyber Security Policies and Strategies: Companies should develop and implement security precautions, policies and procedures to manage cyber risk and govern the protection of data. Companies should ensure constant review of the policies and strategies to suit the digital revolution and technology advanced state that the country is headed.

Cyber-incident Information Sharing and Partnership: Low reporting and information sharing hinders effective measurement of cybercrime. In cyberspace, we need to be constantly looking forward and anticipating challenges through increased co-operation, increased sharing of intelligence and sound risk management, since fighting cyber crime is not a competitive but a collaborative effort.

Investment in Information Security: As we continue to increasingly rely on technology, process automation, centralization of systems and introducing new internet related channels the level of cyber risk is also growing. Companies should invest in information security practices and anti-fraud systems that implement requisite controls to detect and prevent system fraud.

Cyber Security Training and Sensitization: Employees should be trained on a range of security topics to educate them on cyber threats to enable them change poor behaviors relating to ICT and information security and know how to follow the rules, and ultimately reduce the number of breaches due to human error and ignorance.

Building Human Capacity: Companies should ensure that those operating the systems are skilled security personnel and who can be trusted to avoid cases of 'inside jobs'. Trainers also need to churn out talent that can either be hired or that can be enterprising around the Internet economy.

Regular System Audits: Companies should keep vigil online by raising their degree of vigilance and awareness and IT teams are required to invest more time and resources in auditing their entire systems and establishing modalities to reduce breaching incidences both external and from the malicious internal staff.

Cyber Security Response: Creating and testing an incident-response plan. This could include exercises that mimic attacks to highlight weaknesses and plan for responses.

Insurance: Having a policy that pays out appropriately for the breach you experience.

Cyber Risk: An Opportunity for Cyber Insurance

Cyber insurance is an insurance product that protects individual users and businesses from internet-based risks by mitigating losses relating to damage, or loss of information from information technology infrastructure and activities. It mainly covers first-and third-party damage, business interruption and regulatory consequences

Cyber risk insurance market is experiencing rapid development, with the size of global gross written premiums growing from US$850 million in 2012 to an estimated US$2.5 billion in 2014. The United States leads with approximately 90% of the global written premiums in the cyber insurance market valued at US$2 billion in 2014, then Europe, with estimated gross written premiums worth US$150 million.

The global cyber insurance market is expected to expand globally and projected to grow to $5bn in annual premiums by 2018 and at least $7.5bn by 2020.

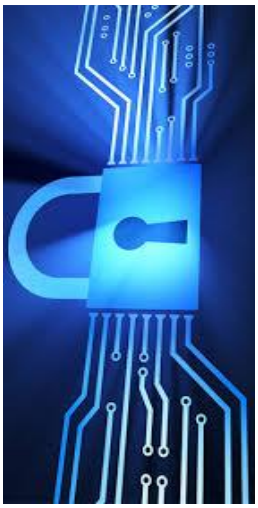
There are about 50 insurers that are writing some cyber coverage globally, the market is dominated by five underwriters: Ace Ltd, American International Group Inc, Beazley P.L.C, Chubb Corp and Zurich Insurance Group Ltd.

In Kenya there is only one underwriter: American International Group Inc.

Main Challenge for Underwriters – Inadequate Actuarial Data

Cyber coverage represents a huge area of opportunity for underwriters, but also presents unique challenges for underwriters as they seek to understand the true nature of the underlying risk.

Many insurance companies have been hesitant to make forays into this market, as sound actuarial data for the cyber exposure is non-existent. Cyber insurance risk is difficult to measure, model and price since reliable actuarial data to model, price, or hedge cyber risk is not available. Metrics for cyber risk are in the early stages of development, and probabilistic models pose high levels of uncertainty, mostly because of the various interconnected activities, between companies, industries and political events; also the external factors that can affect the risk of a cyber-attack such as the industry an organization belongs to, the size and criticality of the company and the region the company is based; This makes neither frequency nor severity predictable.



Hampering the development of this actuarial data is inadequate disclosure regarding cyber attacks by those affected. This situation can be improved if the industry builds a cyber-incident information sharing/data repository, such a repository, including incidents, losses and security profiles, is an important precursor for better predictive algorithms, scores and benchmarks. A data repository will help in building needed actuarial tables, to determine best in class controls, and to improve cyber prediction analytics by studying cyber risk trends over time.

Insurers should coordinate with all parties (corporations, reinsurers, policymakers, technology companies and intelligence agencies) to coordinate risk management solutions, including global standards set for cyber insurance.

Insurance is an important risk-spreading mechanism and an important component of the capital structure of nearly every insurance company but reinsurers have tended to exclude most cyber security risks.

Reinsurers will offer cyber risk once they are confident that underwriters will assume cyber risk in an appropriate way. Robust modeling exposures and potential losses will

provide a better understanding of the evolving threat and could encourage more reinsurance companies to enter the market.

Conclusion

To reduce vulnerability, given the huge volumes of clients' confidential information that they possess, Insurers should invest in cyber security by ensuring they have closely monitored, highly effective cyber security frameworks in place. This will be instrumental in ensuring high customer satisfaction and favorable brand reputation.

Insurers should insist on specific security audits prior to and after issuing an insurance policy, this will help in reducing cyber attack exposures and thus minimize the losses leading to low premium rates that attract more clients. To achieve these insurers should collaborate with cyber security experts who specialize in using technology to deal with cyber vulnerabilities; these will ensure robust cyber risk management to the businesses and organizations insured.

To make cyber-insurance more attractive insurers should provide value-added services such as access to a specialist lawyer, IT forensics experts and crisis management in the event of a data breach.

Insurers have an important risk management and loss control role to play in addressing cyber security and they need to embrace this new frontier taking the necessary precautions and with time as they continue to collect more claims data they will be comfortable to underwrite as they will be able to see trends and patterns emerge.