CENTRAL BANK OF NIGERIA

THE NIGERIA ELECTRONIC FRAUD FORUM (NeFF)

2015
ANNUAL REPORT

NeFF:
Improving and Securing the Cyber-Environment

Foreword

NeFF: Raising the bar in sustaining a safe payments ecosystem

The year 2015 has been very eventful in the Nigerian e-Fraud Forum (NeFF) journey; the Central Bank of Nigeria (CBN) has continued to show leadership in driving NeFF – where Payments Industry stakeholders meet to share experiences on fraud and mitigating factors. This sharing of cyber security intelligence in the financial sector has grown in 2015 and has served as a model for other similar initiatives, not just in Nigeria, but also beyond our geographical entity.

A clear example of what is now known as; "The NeFF Story" is the documented reduction by 46% in attempted fraud while witnessing a 63% reduction in actual losses from 2014 e-fraud figures. These reductions show that fraud was better curbed, and more effective measures were taken to combat fraudsters in 2015.

There is no doubt that in reviewing the performance of NeFF for 2015, the Forum has succeeded in raising the bar of how the unending battle to secure the cyber-space is prosecuted. The landscape for combating e-fraud in Nigeria has changed forever and I am glad that NeFF is driving this change.

The 2015 Annual Report of the Forum has been named; "**NeFF: Improving and Securing the Cyber-Environment**". This shows the importance the Forum accords to improving on co-operation among stakeholders, intelligence sharing and awareness of all consumers of e-products of the threats inherent in embracing advanced payment technologies.

I believe that this report like its forebears, will further shape our collective will in restraining cyber-criminals and creating an even safer payments system, which will impact the growth and development of the Nigerian economy. I therefore commend the report for reading and re-affirm the support of the Central Bank of Nigeria in prosecuting the objectives of NeFF.

Thank You.

Suleiman Barau
Deputy Governor Operations
Central Bank of Nigeria

Acknowledgement

The production of this report was made possible with resource inputs from most of the Deposit Money Banks in Nigeria. A warm appreciation goes to the banks for their contributions.

The Deputy Governor Operations, CBN, Mr. Suleiman Barau has always been there for NeFF, and was of immense support to this project.

Similarly, the Director Banking and Payments System Department of CBN, who also doubles as the Chairman, NeFF, Mr. 'Dipo Fatokun, was a source of great support and inspiration. His enormous support and guidance is sincerely appreciated.

The commitment shown by the Chief Executive Officers (CEOs) of Banks in Nigeria, especially as regards sponsorship of NeFF meetings, was remarkable and therefore worthy of commendation.

Special thanks also go to Messrs Biyi Dosumu, Mohammed El-Yakub, Musa Jimoh, Chidi Umeano, Premier Oiwoh (Chairman CHBO), Tunde Kuponiyi (Chairman CeBIH), David Isiavwe (Chairman ISSAN) and the NeFF Steering Committee members, particularly the review team comprising Joe Obogo, Babatunde Ajiboye, Aliyu Mohammed, Lydia Kuje and John Onuoha, for their commitment and hard work in the production of the 2015 Annual Report.

Disclaimer

The Central Bank of Nigeria (CBN) shall not be responsible for the views expressed by contributors/anthors in this report. No article shall constitute or be deemed to constitute any representation by the CBN.

Therefore, every contributor/author shall be solely responsible for the contents and views in their articles.

Table of Content

The Governor and His Deputies

Godwin I. Emefiele (CON)
Governor

Sulaiman Barau (OON)
Deputy Governor (Operations)

Dr. Sarah Alade (OON)
Deputy Governor (Economic Policy)

Dr. Okwu J. Nnanna
Deputy Governor
(Financial System Stability)

Adebayo Adelabu
Deputy Governor
(Corporate Services)

Chairman's Address for The NeFF 2015 Annual Report

'Dipo Fatokun
Director, Banking & Payments System Department
CBN and Chairman, NeFF

The year 2015 was a sign-post for various cyber-crime activities that showed the evolution of the crime from one often thought to be perpetrated by crude individuals to a higher degree of professionalism and organization. However, to appreciate what we are yet to do, it is important that we understand what we have begun in the course of the year.

We have seen through, the sharp increase in phishing attacks as well as the increased recognition of personal data as high value data. As a Forum, in the course of the year, we have tackled the menace of insider abuse, which has become a conundrum in our fight against e-fraud. Rising from one of our meetings, the need for a coordinated industry fraud desk was mooted. These desks are to act as an industry proactive measure that will reduce the incidence of fraud and limit losses in the face of fraud occurrence.

This has since been implemented via a Central Bank of Nigeria circular to banks, Mobile Money Operators, Switches and all other payment service providers, directing them to maintain dedicated fraud desks in their respective organizations. The impact on electronic Fraud has been massive.

The Forum has also, in the course of the year, embarked upon strategic partnerships with key stakeholders, in the fight against e-fraud. Courtesy visits to the Inspector-General of Police and the Chief Justice of the Nigeria, yielded the first ever Dedicated e-Payment and Card Crime Unit of the Nigerian Police on the one hand and assurances of the Chief Justice of the Nigeria that the Judiciary will stand with the Banker's Committee in providing an effective solution to electronic fraud and other ancillary issues, on the other.

Members of the Nigeria electronic Fraud Forum (NeFF) were also largely represented on a delegation of experts that attended the World Cyber-Security Financial Summit 2015, for the Nigerian Banking Industry, which held in Dallas, USA. This summit afforded our members the opportunity of:

1. Bringing World Class Training to the key bankers of Nigeria
2. Exposing emerging information security threats and how to be prepared.
3. Exposing how banks were being compromised and how to effectively wage the war against e-banking and insider fraud.
4. Learning how to build an effective defence against Cyber-attack and e-fraud.
5. Building a better relationship with the US law enforcement entities (Particularly the FBI)

The Forum also had its maiden retreat from the 21st to 22nd of November, 2015 in Uyo, Akwa Ibom State. Outcomes from the retreat, raised a number of challenges which have been earmarked for confrontation in 2016, and these include;

- Ineffective collaboration with the Nigeria Communication Commission (NCC).
- Duplication of efforts within the industry on issues bordering on payment security.
- Poor industry coordinated awareness campaigns, resulting in people being the weakest link in our payments system.
- Antics of fraudsters through old fraud schemes ,with only variations in their modus-operandi. Some of the fraud trends are Internal Fraud Compromise; Third Party Payment Application Compromise; Identity Theft/Account Compromise; Phishing Sites; Skimming; Rogue Mobile Application; Physical Theft; Rogue Merchant and Other Points of Compromise.
- Proliferation of Phishing attacks on unsuspecting customers
- The latest fraud trend of DDoS attack also known as Ransomeware.

It is therefore a deliberate attempt to reflect in our 2015 NeFF Annual Report, a compendium of our activities in the course of the year, that we have aptly captured our 2015 theme; "NeFF: Improving and Securing the Cyber-Environment".

Looking forward and moving ahead, as a Forum, we have a mandate to ensure that the confidence in our Payments System is not compromised. In the face of rapidly changing threats, we have needed to act, and so we have. In the light of what lies ahead, we no doubt would be busy in 2016, because even though we have come thus far, there is still a lot that remains to be done.

As usual, we depend on the support and continued patronage of our stakeholders in ensuring a safer and more secure Payments System. We have remained a platform for restoring public confidence in our payment channels and we will continue to impress on our mandates, we will not let the steam down, rather, we will up the ante, to deliver a credible, reliable and efficient payments system for Nigerian banks and their various stakeholders.

The unveiling of the 2014 NeFF Annual Report

Aggressive Consumers Awareness Initiatives: A Proactive & Consistent Mechanism to Preventing E-fraud.

By

Onajite Regha.

CEO, Electronic Payment Providers Association of Nigeria (E-PPAN)

Onajite works in several committees in the financial industry and writes in several publications. She serves on the board of various companies. Also serves on several committees of payment system in Nigeria and in ECOWAS sub-region. She contributes to several publications and has authored and co-authored several policy briefs, focus notes, white papers etc and has traveled wide in pursuit of furthering the electronic payment businesses in Africa. Onajite is widely consulted on issues of e-payment in Nigeria and Africa. is also is a member of the advisory board of Aitec West Africa Conference. She is currently the Executive Secretary/CEO of the E-Payment Providers Association of Nigeria.

With the growth in the use of electronic payments, criminals have found yet another means to increase their nefarious ways of fleecing innocent victims of their money. They employ methods such as counterfeiting, identity theft, card trapping, pharming, cloning, malware attack, BIN attack, skimming, phishing and carding to defraud and steal from users of electronic payment. Simple consumers are not the only targets of electronic payment crimes, other targets include the merchants; retailers; banking institutions; organisations that use individuals' data to transact businesses and even the government. No possible target is spared by these criminals.

Payment fraud is described by Bigcommerce Enterprise as any type of false or illegal transaction completed by a cybercriminal. The perpetrator deprives the victim of funds, personal property, interest or sensitive information via the Internet. Payment fraud is characterized in three ways: Fraudulent or unauthorized transactions; Lost or stolen merchandise; False requests for a refund, return or bounced cheques.

The consequences of the criminals' activities are numerous and can be devastating to the victims of such crimes. These can involve one or more of the following: the painful loss of moneys of victims of such crime, the socio-economic impact of erosion of confidence in the national payments system and the psychological trauma the victim faces. A research by Weizmann Institute scientists reveals that financial loss can lead to irrational behaviour and may also have implications for traumatic stress disorder (Rony Paz, 2012).

According to SpamLaws.com, the emotional effects fraud can have on a victim are perhaps the most troubling. In comparison to victims of violent crimes, e-payment crime victims are susceptible to many stress-related complications and psychological problems. When fraud evolves into an even more damaging crime such as identity theft, many victims find it difficult to recover from the financial loss. If they were baited into a scam, they may feel as if they not only lost their money, but their sense of security, self-esteem and dignity as well. For some, this may be an ordeal that takes years to resolve. A fraud victim may feel lonely or embarrassed because of a change in social status. The incident may cause marital problems and prevent someone from providing adequate support for their family. Sadly, the social indifference behind this type of crime can be reflected on the law to some extent. (Sorkin)

Electronic payment crime can impact greatly on a country and its economy. It can result in direct economic decline due to a reduction in patronage of public facilities using electronic payment, and indirect economic losses endured by corporations contributing to the National economy. Electronic crimes can bring a country to its knees if not properly managed.

To eradicate the consequences of electronic fraud, there need to be concerted efforts to fight fraud collaboratively. Currently in Nigeria, like everywhere else in the world, stakeholders are coming together to fight fraud. A lot of initiatives and various networking platforms have sprung up to tackle the issues of electronic payment crimes. Stakeholders, especially payment providers are making great efforts to invest in the right technology, and to implement the right processes that can eradicate the ugly trend. But we all know that fraud cannot be completely eradicated. Currently, the activities that are being carried out are only best efforts to reduce the level of electronic fraud to possible minimum.

Fraudsters depend on their loots for survival, and will therefore not give up as stakeholders make efforts to stop them. They will continuously re-invent themselves and their modus-operandi to remain in business. The rapid evolvement in technology gives them an impetus to continue to remain one step ahead of efforts to deter them. They thus latch on new technologies and methods to attack unsuspecting victims.

While payment providers make tremendous efforts to block these fraudsters, consumers, majority of them in ignorance, make nonsense of these investments of the payment providers by making themselves easy preys to the fraudsters. Investigators of e-fraud are shocked to find consumers fall to very simple tricks employed by the fraudsters. It therefore behoves on the custodians of the payment system and the payment platform providers to protect the consumers and users of the systems, by increasing their knowledge on how electronic crime works. Presently, the consumers represent the weakest point of the payment chain.

A proactive way to prevent fraud from happening through the consumer is to invest in awareness initiatives targeted at driving behavioural changes and promoting the culture of security consciousness among consumers. Consumers' behaviours are driven by cultural, social, personal and psychological factors. Among the factors influencing consumer behaviour, psychological factors can be divided into 4 categories: motivation, perception, learning as well as beliefs and attitudes. Beliefs as well as attitudes are generally well-anchored in the individual's mind, and are difficult to change. For many people, their beliefs and attitudes are part of their personality and of who they are. (Perreau). To change consumers' behaviour, messages of security awareness must be exposed to the consumers in a consistent and proactive strategy.

To achieve a national shift in behaviour as it regards to consumers attitude to safe payments, the entire stakeholders in the National payment system must shun brand and silo arrangements and move to fit into the bigger picture possible under the central government, to tackle the

problem of ignorance displayed by consumers. It has been said several times over, that fraud is not a basis for competition. A massive awareness creation can be very expensive if borne by single entities and solo arrangements which will almost guarantee failure.

The level of investment that has gone into technology and processes to curb fraud is quite commendable, but such investments also need to be made in the users and consumers of the payment products. Awareness creation should go beyond merely providing the information to those who care to know. It should be a deliberate effort to inform all users irrespective of their state of mindfulness. Stakeholders therefore have to employ a mix of strategies to catch the attention of the most uninformed user. There should be a strategic aggressiveness to the creation of awareness to match the ferocity employed by the criminals in attacking unsuspecting consumers.

An aggressive awareness campaign like most successful marketing (or sales) campaigns must target consumers in two folds, above the line and below the line. Above the line (ATL) sales promotion is a type of advertising through media such as television, cinema, radio, print, and Out-of-home to promote brands or convey a specific offer. This type of communication is conventional in its nature and considered impersonal to customers. Below the line (BTL) advertising on the other hand, seeks to reach a consumer (instead of a mass audience) directly rather than through an intermediary. This type of advertising is often centred on specific localities. Commonly, it includes direct mail campaigns, trade shows and catalogues; this advertising type tends to be more focused.

During the introduction of the Cashless Nigeria Initiative, E-PPAN, under the auspices of the Central Bank of Nigeria, in collaboration with the providers of electronic and mobile payments platforms, engaged the Nigerian Citizenry in an effective campaign for the adoption of electronic payment channels. Despite the challenges posed by the poor infrastructure, the adoption rate by Nigerians was an attestation of an effective campaign system which employed above and below the line marketing strategy. For more information, you can refer to the 2014 Cashless Nigeria Report (Published by E-PPAN).

For a consumers' fraud awareness campaign to be successful, we have to understand that awareness creation must rely on the concept of effective frequency. What this means is that the message has to be exposed to the consumers multiple times, to catch their attention. There are various schools of thoughts on how many times a message must be repeated to get the

attention of the average listener for behaviour to be altered. This ranges from seven to twenty two times. However, one common factor that underlies all positions is that, it must be consistent and frequent. Agreed that this can be expensive, but like a popular saying that goes thus “if education is expensive, try ignorance”. The cost of sustaining ignorant consumers who fall easy prey to the antics of cybercriminals far outweighs the cost of a unified strategic awareness creation supported by the full gamut of the financial industry.

In this age of media and message oversaturation, it is advisable to have a good blend and mix of above and below the line channels. While E-PPAN carried out the awareness campaign of the Cashless Nigeria Initiative, we discovered a system of influence which we tagged as the “Pyramid of influencers”. These influencers include the government (especially local government), the media, the religious leaders, learning institutions, traditional and community rulers, the trade and market leaders, and peers. To successfully carry out a campaign against fraud, the power of these influencers should be brought to bear.

In summary therefore, my advice will be that the industry has to, as a single entity, engage aggressive consumers' awareness initiatives as a proactive & consistent mechanism to preventing e-fraud. The campaign must be a focused campaign across all channels carrying the same uncomplicated message. According to David Plouffe, Barack Obama's 2008 campaign manager, “We live in a busy and fractured world in which people are bombarded with pleas for their attention. Given this, you have to try extra hard to reach them. You need to be everywhere. And for people you reach multiple times through different mediums, you need to make sure your message is consistent. Messaging needs to be aligned at every level.”

REFERENCES:

- Weizmann Institute of Science. "Losing money, emotions and evolution." Science Daily. Science Daily, 12 June 2012.
- https://www.bigcommerce.com
- http://theconsumerfactor.com/en/4-factors-influencing-consumer-behavior/
- Below The Line Advertising Definition | Investopedia
  http://www.investopedia.com/terms/b/below-the-line-advertising.asp#ixzz43cuzl3OB
  http://www.mrmediatraining.com/2013/12/10/how-many-times-should-you-repeat-your-messages/#sthash.eSiPvNLP.dpuf

Cybercrime (Prohibition, Prevention, Etc) Act, 2015: Implications to Individuals and Financial Institutions

By

IBRAHEEM ADEKA ATUKPA

Financial Policy and Regulation Department

Central Bank of Nigeria, Abuja

Ibraheem Adeka Atukpa works at the Central Bank of Nigeria in the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Division of the Financial Policy and Regulation Department. He had worked in Human Resources Department and Security Services Department of the Bank.

Mr. Atukpa holds the following qualifications: Barrister-at-Law (BL), from the Nigerian Law School, Kano, LL.B (Uni-Abuja), Master's Degree in Industrial and Labour Relations (MIRL) from University of Maiduguri, HND (Business Administration) from Yaba College of Technology, Yaba-Lagos. He is an Associate Member of International Federation of Protection Officer (IFPO), USA; Associate Member of Certified Anti-Money Laundering Specialist (ACAMS); Associate Member of the Association of Certified Fraud Examiners (ACFE); Member, Nigerian Institute of Management (Chartered).

1.0. Introduction

The evolution of electronic payments system has made financial transactions easy and life more interesting as financial transactions can be made at the comfort of one's home or office or "on-the-go". Payments system platforms are made accessible courtesy of internet banking where so many electronic devices (computers, mobile phones, etc) are deployed to make financial transactions simple, efficient and effective. But, all of these are not without sunny sides because the internet is a cyberspace accessible to the user without some sort of restrictions. Therefore, organisations try to build firewalls around their platforms to restrict or deny access to unauthorized users. Firewalls notwithstanding, electronic fraudsters do "wake-keep" to device means to break the walls and defraud organisations and people.

Cybercrime (Prohibition, Prevention, etc) Act, 2015 was enacted on the 15th May, 2015 as a response to the necessity to address cybersecurity challenges; and to criminalise unauthorized access to the nation's Critical National Infrastructures and businesses.

The Objectives of the Act are provided in Section 1(a-c). It states: "*The objectives of this Act are to –*

(a) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria;

(b) ensure the protection of critical national information infrastructure; and

(c) promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights".

2.0. Implications to Individuals

Freedom of Expression: Section 39(1) of the 1999 Constitution of the Federal Republic of Nigeria (as Amended), entitles every person(s) in Nigeria the freedom to express himself or herself in these words, "*every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without*

interference". There is nothing in these words that suggest the use of unprintable and vulgar language, direct abuse or words that impugn on the integrity of a person, a group, a tribe, a religion or even a region. This is not contemplated in the provision because there is limitation to the extent one uses his right or freedom of expression. For example, section 24 of the Cybercrime (Prohibition, Prevention, etc) Act, 2015, provides extensive provisions covering varied aspects of electronic communications, particularly section 24(1)(a) & (b). It states: "*A person who knowingly or intentionally sends a message or other matter by means of computer systems or network that –*

(a) is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent, or
(b) he knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent, commits an offence under this Act and is liable on conviction to a fine of not more than N7,000,000.00 or imprisonment for a term of not more than 3 years or both".

Section 26 of the Act also provided for racists and xenophobic offences, including offences of harassment, threat to persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion. Committing or supporting acts constituting genocide or crimes against humanity is prohibited and punishable under the Act.

Learning points from the provisions of section 24(1)(a) & (b) and section 26 are to the effect that: How have you been using the computer system assigned to you for your official duty? Are you mindful of the kind of messages you send or receive? Beware! You may be falling foul of the Law which will qualify you for prosecution under the Act. Note that under the Act, a computer system:

(a) refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated or interactive processing of data;
(b) covers any type of device with data processing capabilities including computers and mobile phones;
(c) consists of hardware and software which may include input, output and storage components that may stand alone or be connected in a network or other similar devices; and
(d) includes computer data storage devices or media.

What this means is that those mobile phones (especially smart phones) at your disposal could be an albatross if not properly manipulated or operated in line with the provisions of the Act. It is therefore surprising that some members of the National Assembly who enacted the Cybercrime

Act in May, 2015 were proposing a bill to enact a law to regulate social media. One wonders what will be the content of the bill that would not have been taken care of by virtue of S.24 (1)(a) & (b) and S.26. Some of the Senators who moved the motion for the enactment of a law that would regulate social media communication were not "first-timer" Senators. It was unnecessary and would have been counter-productive. We need to read and understand our Laws!

3.0. Implications to Financial Institutions

Before the Cybercrime (Prohibition, Prevention, etc) Act, 2015, the Central Bank of Nigeria (CBN), had its Information Technology (IT) Policies which prohibited some of these crimes as contained in the Act. Of particular interest and relevance to this paper is the Email Acceptance Usage Policy which outlined what to do, what not to do and the consequences of a breach. A phrase in the Policy reads: "Users shall not send mail messages that carry malicious content, provocative, ethnic, racial discrimination or other profane content" (CBN IT Policy document, pg7). This conveys the spirit of the provisions in section 24 of the Act.

Section 37 of the Act chronicled the duties of financial institutions in the course of electronic financial transactions or transfer.

(a) Verification of Identity of Customer

(b) Sub-section 1(a) requires financial institutions to verify the identity of their customers before carrying out electronic financial transactions. (Also, see Regulation 14 and 15 of the CBN AML /CFT Regulations, 2013, and Section 3 of the Money Laundering (Prohibition) Act (MLPA), 2011 (as amended) on verification of identity of customers).

(c) The Principle of Know Your Customer (KYC)

Sub-section 1(b) of the Act places on the financial institutions the duties of applying the principle of know your customer in documentation of customers before execution of the transactions. [See also Regulation 13 of CBN AML/CFT Regulations, 2013 and Section 3 of MLPA, 2011 (as amended)].

(d) Unauthorised Debit on Customers' Account

Sub-section 3 provides that any financial institution that makes an unauthorized debit on a customer's account, the financial institution shall reverse it within 72 hours upon a written notification by the customer. Failure to reverse the debit within the stipulated hours attracts restitution.

Any financial institution that fails to perform its duties in line with the provisions of Section 37 of this Act, is liable on conviction to a fine of N5,000,000.00, including restitution of the debit in the case of failure to reverse the debit within the stipulated timeframe.

4.0. Conclusion

A good understanding of the Cybercrime (Prohibition, Prevention, etc) Act, 2015; Money Laundering (Prohibition) Act, 2011 (As amended); the CBN AML/CFT Regulations, 2013; and Information Technology Policies of our various institutions will guide our behavior on how to use the devices or computer systems at our disposal. If they are properly used in line with the extant laws, regulations and policies, they will impart our lives positively. On the contrary, if they are used otherwise we may be breaking the laws and may eventually face the full consequences of our actions or inactions.

REFERENCES

- CBN AML/CFT Regulation, 2013
- Cybercrime (Prohibition, Prevention, etc) Act, 2015
- Information Technology Policy document of the Central Bank of Nigeria (2015)
- Money Laundering (Prohibition) Act, 2011 (As amended)
- The 1999 Constitution of the Federal Republic of Nigeria (As amended)

E-Fraud in Nigeria: Growing or Dying Trend

By

Osita Nwanu, CISA, CISM, CEH, OCP
Head, Systems Control & Business Continuity Management
First City Monument Bank Limited

Osita Nwanu, CISA, CISM, CEH, OCP, OCA, ITIL, is currently the Head, Systems Control & Business Continuity Management at FCMB Limited. He leads the fraud, IT control, information security and business continuity teams of the bank.

Osita has over 13 years' experience in information technology, internal audit and internal control within the Nigeria banking environment. His previous work experience was with Computer Warehouse Group and First Bank Nigeria Plc. Osita holds a bachelor's degree in Computer Science from University of Uyo and an MBA from University of Lagos.

Introduction

In spite of the challenging economy, the use of e-channel platforms –Internet banking, Mobile banking, ATM, POS, Web, etc. has continued to experience significant growth. According to NIBSS 2015 annual fraud report, transaction volume and value grew by 43.36% and 11.57% respectively compared to 2014.

Although e-fraud rate in terms of value reduced by 63% in 2015, due, in part, to the introduction of BVN and improved collaboration among banks via the fraud desks; the total fraud volume increased significantly by 683% in 2015 compared to 2014.

Similarly, data released recently by NITDA (Nigeria Information Technology Development Agency) indicated that Nigeria experienced a total of 3,500 cyber-attacks with 70% success rate, and a loss of $450 million within the last one year.

The sustained growth of e-transactions as depicted by the increased transaction volume and value in 2015, coupled with the rapidly evolving nature of technology advancements within the e-channel ecosystem continues to attract cybercriminals who continuously develop new schemes to perpetrate e-fraud.

What is e-fraud? What is responsible for its growth in Nigeria? What are the major techniques used by these criminals to commit fraud? Is e-fraud dying in Nigeria? Can it be mitigated?

What is e-fraud?

e-fraud can be briefly defined as online trickery and deception which affects the entire society, impacting upon individuals, businesses and governments.

Why Is It Growing?

The following inherent factors fuel e-fraud in Nigeria:

- Disgruntled staff;
- Increased adoption of e-payment systems for transactions due to its convenience and simplicity;

- Emerging payment products being adopted by Nigerian banks;
- Growing complexity of e-channel systems;
- Abundance of malicious code, malware and tools available to attackers;
- Rapid pace of technological innovations;
- Lax security practices and knowledge gap;
- Anonymity approach of the internet;
- The increasing role of Third-party processors in switching e-payment transactions;
- Siloed approach to fraud detection and prevention;
- Lack of inter industry collaboration in fraud prevention -banks, telcos, police, etc.

What are the Major Techniques?

Cybercriminals employ several techniques to perpetrate e-fraud, including:

- Cross Channel Fraud: customer information obtained from one channel (i.e. call center) and being used to carry out fraud in another channel (i.e. ATM).
- Data theft: hackers access secure or non-secure sites, get the data and sell it.
- Email Spoofing: changing the header information in an email message in order to hide identity and make the email appear to have originated from a trusted authority.
- Phishing: refers to stealing of valuable information such as card information, user IDs, PAN and passwords using email spoofing technique.
- Smishing: attackers use text messages to defraud users. Often, the text message will contain a phone number to call.
- Vishing: fraudsters use phone calls to solicit personal information from their victim.
- Shoulder Surfing: refers to using direct observation techniques, such as looking over someone's shoulder, to get personal information such as PIN, password, etc.
- Underground websites: Fraudsters purchase personal information such as PIN, PAN, etc. from underground websites.
- Social Media Hacking: obtaining personal information such as date of birth, telephone number, address, etc. from social media sites for fraudulent purposes.
- Key logger Software: use of malicious software to steal sensitive information such as password, card information, etc.
- Web Application Vulnerability: attackers gain unauthorized access to critical systems by exploiting weaknesses on web applications.
- Sniffing: viewing and intercepting sensitive information as it passes through a network.
- Google Hacking: using Google techniques to obtain sensitive information about a potential victim with the aim of using such information to defraud the victim.
- Session Hijacking: unauthorized control of communication session in order to steal data or compromise the system in some manner.

- Man-in-The-Middle Attack: a basic tool for stealing data and facilitating more complex attacks.

Is e-fraud Dying?

Fraud value may have reduced in 2015, but the significant increase in volume of attacks depicts the enormous threat of e-fraud. Furthermore, information released by security firm, Kaspersky, shows that in 2015, there were over a million attempted malware infections that aimed to steal money via online access to bank accounts.

As financial institutions adopt emerging payment systems and other technological innovations as a means of increasing revenue and reducing costs; cyber thieves on the other hand, are exploiting gaps inherent in these innovations to perpetrate fraud bearing in mind, the fact that *security is usually not the primary focus in most of these innovations*.

Can it be mitigated?

Because of the risk inherent in the e-channel space, many organisations have attempted to implement the following comprehensive strategies for detecting and preventing e-fraud:

- Fraud Policies
- Fraud Risk Assessment
- Fraud Awareness and Training
- Monitoring
- Penetration Testing
- Collaboration

Conclusion

Increased revenue, optimized costs, innovations, regulation, convenience and simplicity are the major factors driving the massive adoption of e-channel platforms in Nigeria. Furthermore, the usage of these platforms have created opportunities for cyberthieves who continuously devise new and sophisticated schemes to perpetrate fraud.

e-fraud will continue to grow, and combating it requires effective fraud strategies, collaboration and cooperation of many organisations in Nigeria including government agencies and other countries. If otherwise, cybercriminals would be getting richer from the hard work of others due to lack of united front on the part of everyone.

NeFF visit to the Inspector General of Police

Faces at the CJN's Visit

The Rise of Digital Payments

By

Deji Oguntonade

Deji holds a Bachelor of Science Degree (1989) in Chemical Engineering from the University of Lagos and an MBA in Information Technology from Federal Universtiy of Technology, Akure (FUTA). He has attended various courses in Nigeria, Switzerland, India, London, Singapore and South Africa.

Deji Started his Banking career in 1991 with Guaranty Trust Bank Plc, and subsequently also worked in for Equitorial Trust Bank and First Inland Bank Plc. His Banking experience has spanned Operations, Marketing and Information Technology and E- business.

Deji's major area of focus/interest is developing/deploying electronic payment solutions as a competitive tool in the banking industry. Since 2001, Deji has pioneered several cutting-edge and award winning Technology products that are in application nationwide. Of major significance are Internet Banking, Mobile Banking and FlashMeCash

Deji's major strengths are innovation, human capital development and a never say die attitude. He makes a positive impact on the lives of those he has encounters with and he is a role model for many players in the Financial and Information Technology Industry.

As the end of the month approaches, the frenzy of satisfying payments due commences. In addition to meeting due commitments, which range from salary payments, custom duty payments, replenishment of telephone airtime, to vendors payments, the average business owner is also saddled with the headache of preparing schedules, writing cheques and other paperwork to vendors, completing custom duty payment paperwork, as well as ensuring that required signatories are available to authorize necessary payments.

Further complicating the payment process, all required variables to ensure successful payments must be available at the end of every month, and often within short notice. In the event that a key signatory is out of town, all payments will be placed on hold till he returns, which could result in severe loss of income and in extreme cases, bring the entire operations of the company to a halt. After the business executive has properly executed all processes and documentation required to make payments, and has submitted duly completed payment documents and instruments to the bank, the payments are still subject to the risks of verification time, clearing time, delayed payments, reconciliation issues and bank errors, all of which cost the business time and efficiency, ultimately resulting in reduced profits.

Every cloud has a silver lining

The advent of electronic banking has allowed companies do business at speeds never before possible. It has also given rise to new opportunities and efficiencies that were not possible just a few years ago. A business looking to deploy an e-banking solution can primarily use it either to gain cost efficiency or as an avenue for revenue collection. Fortune, they say, favours the prepared mind. The fortunes of a business executive who has taken the time to explore the options and available features of electronic banking, are very different from the previously discussed executive. For example, the GTBank Automated Payment System (GAPS) possesses features which allow real-time automation and administration of salary payments, vendor payments, FX transfers to local and foreign parties, scheduling of payments at future dates etc. GAPS allows for remote approvals by authorised Signatories who can authorize transactionsfrom their mobile devices. The rigours of reconciliations are quelled as payments can be processed either as “Single debit, Multiple credit” or “Multiple debit, Multiple credit” to

make the statements of accounts tidy and easy to understand. Transactions reporting on GAPS features customizable reports, provided to keep track of all transactions and ensure a seamless user experience. The payment system also allows you to store details of the beneficiaries therefore making recurrent payments easier. For most companies, supporting documents are required for all payments. With GAPS, these supporting documents can be uploaded as part of the payments so the approvers wherever they are, can download and view the supporting documents before authorizing the transactions.

Cost and other Efficiencies

The cost of an electronic payment is a fraction of the cost of processing a payment at a 'Brick & Mortar' location. In addition to obvious cost savings, electronic banking provides time savings, and increased operational efficiencies. An added and often overlooked benefit to electronic banking is the goodwill generated towards the recipient who is grateful to receive instant payments devoid of inconvenience and logistical nightmares.

Income generating strategy

Customers with regular receivables can automate their collections through the use of Direct Debit. Direct Debit allows organizations such as Insurance companies, Credit and thrift societies, collect monthly contributions without visits to the customer or bank branch. A mandate sent to the bank electronically is all that is required to kick-off the process. This guarantees the timely receipt of income as beneficiaries are credited automatically.

Have you ever imagined how the fortunes of your business can change if you can automate your payments and collections to consummate on set dates?

Corporate organisations and Small and Medium Enterprises (SMEs) can subscribe to the Guaranty Trust Automated Payment System (GAPS & GAPS Lite) an Internet Banking product that is designed to meet the varied remote banking needs of corporate organisations and SMEs. It is highly secure and customizable and is easily adapted to the need of the discerning customer.

Improving Security of Our Cyber-Environment

By

Ighoakpo Eduje,

Information Systems Security, Access Bank Plc.

Ighoakpo Anthony Eduje is a seasoned Information Systems Security professional with over sixteen (16) years banking experience spanning across, Information Systems Security, Audit, Risk Management, Control and Compliance. He is currently the Head, IT & E-Business Conduct and Compliance in Access Bank Plc responsible for Information Systems Security, IT & Channels Conduct and Compliance. He has a Bachelor's degree in Computer Science from the University of Benin, Benin City, Nigeria, and also attended the Middle Management Programme at the prestigious Wharton School of The University of Pennsylvania, USA

He is a Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), ISO27001 (Information Security Management System) Lead Implementer and Auditor, ISO22301 (Business Continuity Management System) Lead Implementer, ISO31000 Risk Management, Payment Card Industry- Internal Security Assessor (PCI – ISA), an Oracle Certified Associate (OCA), a Certified Ethical Hacker (CEH), and Computer Hacking Forensics Investigator (CHFI).

He served on the Board of ISACA (Lagos Chapter), also served on the Executive Committee of the Information Security Society of Africa (Nigeria), and currently a member of Information Security and Risk Management Initiative Working Group, under the Payments System Vision 2020 (PSV2020) project.

As our economy gets larger and our institutions have greater international presence, the nature and extent of cyber risks will continue to expand. Recent cases of man-in-the-middle attacks, ransomware, e-mail spoofing/masquerading, phishing, social engineering, and even cases of DDOS attacks in our cyberspace, give cause for concern. In addition, social engineering attacks in the form of; phishing, vishing, smishing, which play on the victims' emotions or intelligence have soared in our cyberspace within the last few months.

In the last few weeks, a phishing mail made the rounds and read thus "… According to our records, you are registered for our customer digest monthly bulletin and this comes with a charge of N10,050.00 we will like to ask you to confirm this on the link < phishing site url> if you wish to reject the registration follow the reference <phishing site url>". Several customers who were already angered by the N50 stamp duty unleashed their emotions by voluntarily giving away their online transaction credentials on the phishing sites, only a few ….only to call their bank's contact centre and fraud teams to complain that unauthorized transfers had been done on their account after they rejected "customer digest monthly bulletin".

Customer awareness is the only reminder that can hold back such angered customers from clicking on anything just to vent such emotion.
While it is obvious that the Central Bank of Nigeria (CBN), Financial Institutions and other stakeholders are emplacing various security measures to fight fraud and cybercrime, the issue of collaboration and continuous review and improvement among stakeholders cannot be overemphasized.

It is also key to continuously benchmark infrastructure and systems against leading best practices in cyber security, encourage improved response to evolving threats and work closely with telecommunications firms, internet service providers, regulators and law enforcement agencies and other stakeholders.

Customer awareness is a very critical issue that must be addressed on a regular basis and handled with heightened sensitivity, until customers know that they are responsible for protecting themselves and their financial assets from fraud plied through social engineering.

This write up highlights a few do's and don'ts to stakeholders with a mini social engineering quick check.

Every customer should:

- Keep his/her online transaction credentials (User ID, Password, token/PIN) confidential
- Never submit his/her online transaction credentials in response to any mail or links.
- Only use his/her online option when consuming a transaction initiated on a valid site at your own instance.
- Never install a payment applications sent through e-mail. Such apps should be installed only from the online stores e.g. Appstore, Playstore, Googlestore etc.
- Report any bank official who requests, via e-mail, SMS or voice message, his/her online transaction credentials.

Financial institutions should ensure:

- Fraud awareness as part of customer onboarding
- Dedicated email address and contact phone numbers are availed to customers to report all suspicious activities
- Active collaboration with stakeholders to combat cybercrime and fraud
- Continuous review and security upgrade of its platforms, solutions and services

Regulators should:

- Drive the forum/platform for collaboration among stakeholders
- Drive improved compliance with global security best practice and regulations.
- Encourage shared platforms/services to reduce the cost of continuous security
- Sponsor regular customer information security awareness jingles and publications

The government should ensure:

- Establishment and equipping of Special Cybercrime unit within the Police Force
- Integration of the BVN platform into the NIMC system for easy tracking of cyber criminals

Creation of legal framework to promptly prosecute cybercriminals.

Ransomware: An Evolving Threat

Olusola O. Olodude

Mr. Olusola Olodude is a staff of Nigeria InterBank Settlement System Plc (NIBSS). He holds a B.Tech degree in Computer Engineering from Ladoke Akintola University of Technology, Ogbomoso and a Masters in Computer Systems from the University of Ibadan, Nigeria. Olusola joined the service of NIBSS in March, 2008. He has worked in various departments of NIBSS which includes Switching Operations, Nigeria Automated Clearing System (NACS) and Support Services. He was the team lead, Operation Support Unit of NIBSS before his redeployment to Fraud Management. He is currently the Head of Fraud Management Unit. He has facilitated in several training on Electronic Fraud and has serve as guest speaker in several fora within the industry.

Olusola is highly experienced in Electronic Payment Operations, Cyber-Security, Fraud Detection & Prevention and Investigation. His certifications include Certified Fraud Examiner (CFE), Certified Ethical Hacking (CEH) and Computer Hacking and Forensic Investigation (CHFI). He is an associate member of Association of Certified Fraud Examiners (ACFE). He is also a member of Nigeria Electronic Fraud Forum (NeFF) and Nigeria Computer Society (NCS).

ABSTRACT: Growing up in the south western part of Nigeria, I almost do not know the meaning of the word kidnapping. As I grew up and technology increases and mass media evolve with the outbreak of social media, the consciousness of kidnapping became real. Many countries fighting insurgency have their share of kidnapping at various levels. Their victims are subjected to various inhuman treatment, just to get their loved ones pay levied amount placed on their treasured life. Our world today is electronic in nature. Everything from payment, automobile, teaching, medicine and so on is moving from the traditional mode to electronic operations. So also kidnapping. This time, not the physical human being but your computer files and records. Wait a minute!!! How do you feel when you lost your mobile phone? Sad, because of the cost of the phone – maybe not. You will think about your information - contacts and messages. God help you if you do not have a backup. Computer malware has evolved over the years, and what we have today is Ransomware. This is the type of malware that finds its way into your computer system, encrypt all your files and locks up your system. You are requested to make a payment if you love your files. At this point you feel empty, you are about to lose something dear to your heart. YOUR FILES HAVE BEEN KIDNAPPED!!!

KEYWORDS: Ransomware, Kidnapping, Malware, Encryption

1.1 Ransom and Kidnapping: The Traditional Way

- Kidnapping is a global phenomenon that has frequently occurred in many parts of the world. The Oxford Advanced Learners Dictionary has defined kidnapping as abducting and holding anybody captive, typically to obtain ransom. Some kidnappers are happy to receive a ransom, while others may hold their captives longer to make more demand from the relatives of the victim.

- Today, the word "Ransom" has become a common word in Nigeria as Kidnapping is becoming a lucrative business. From the south to north, east to west, the occurrence of kidnapping has become a trending news. Even little children are not spared in this horrible and terrific menace. These kidnappers consummate their action for financial gain, while some, is to drive home a point. Some perpetrate this act to tarnish the image of government of the day. The kidnappers makes cool cash by taking their hostage to a secured location and asking for a huge sum of money to be paid as ransom. It is a pathetic situation to have your loved ones in captivity, and only a huge sum of money could assure the release of such a fellow from the dungeon.

1.2 Ransomware: The digital Kidnapping

- Ransomware is a combination of ransom and software, and refers to any type of malware that demands payment in exchange for the return of a 'kidnapped' file. This threat works just like a real life kidnapping, except the kidnapped here are your files. This can include multimedia files, system files, or office files that you rely on for your day-to-day activities. Ransomware is a type of computer malware. This is a malware that hinders or prevents the real users from accessing their files on their computer. It rather compels people to make payments through an online platform before they could have access to their files. It is an operation spread by syndicates who want to make quick money. Upon successfully infecting your computer, or locking your files, they demand that you pay some amount of money. The distinct line of separation between an ordinary malware and a ransomware is the potential of a ransomware creator to exploit their victims, and pressurising them to make payment. In some cases, this malware will function more like a "scareware", by displaying pop-up(s) such as "You have been infected with a virus, please make a purchase product (XYZ) to fix your computer". The malware can even allege you to have downloaded illegal files, or accuse you of child pornography and mandate you to pay a fine before you can continue your computer usage. Some ransomware will offer you a candid advice. "You observed your computer seriously been infected and pop-up(s) over your interface will only go away if and only if you pay such amount of money to us".

- Today, Ransomware operations is becoming more increasingly sophisticated. Immediately the malware infects your computer system, it automatically initiates the encrypting of your files. This will prevent your access to your own very files or data if you don't have the encryption key. Immediately your files are locked up, you will be informed that your files have been locked. You have to pay $500 to gain access to your file. After

paying the required amount, they send you the key to unlock your file.

1.3 Ransomware: The Types

- We have two main forms of ransomware:
- These are Locker ransomware and Crypto ransomware.
- Locker ransomware:

The locker ransomware is a malware with the capacity to deny user access to system resources. The ransomware is empowered to lock a user interface, thereby demanding a fee to restore rights. The lock in this sense could affect the mouse from working or provide limited operations of the keyboard. It may only grant the privilege to enter the payment code given in some instance. Basically, what this type of ransomware does is to prevent its victims from accessing their system interface. It does not affect the files. The lock ransomware can be overcome. It is less effective as it can be removed by simply restoring your computer to its original state. Since this type of ransomware is less destructive and can be easily removed, it always employs various intimidating techniques that will submit its victim into paying the ransom. The threat sometimes employs psychological method to trick you into paying. In some cases, the lock screen turns on your camera which creates a feeling that someone is watching you. Sometimes, the message on the interface reveals that of a law enforcement agency stating that the authorities have fined you for an offence. The ransomware creators may claim they found evidence of child abuse, bestiality, usage of pirated software or perhaps, stating that you have visited illegal website. However, it is important to note that this type of ransomware is more devastating in wearable devices and the trending Internet of Things (IoT) where several connected devices can be at risk with limited interacting options for victims.

- Crypto ransomware:

From the name, Crypto ransomware is more devastating as it is empowered to locate and encrypt valuable data stored within a computer system. This is done by encrypting the victim's files using an encryption algorithm. Modern ransomware employs such a strong

encryption algorithm that encrypts without the knowledge of the user. The encrypted files remained inaccessible and unusable for the user. Upon successful infection, the crypto ransomware silently looks for your treasured files and gets it encrypted. The ransomware continues its operations by quietly looking and encrypting all valuable data to the user before confronting its victims with the data lock message. "With most crypto ransomware infections, the affected computer continues to work normally, as the malware does not target critical system files or deny access to the computer's functionality" (Symatec). In this case, the user still utilizes the computer and can perform some functions without access to the encrypted files.

- The ransomware makes the data inaccessible to its owner unless the user is ready to buy the decrypting key. You can imagine your data was kidnapped and here comes the pop up "please pay $400 to unlock your data". Today's world is changing, and every part of our lives is becoming more digital, including our day-to-day activities. Almost every part of our lives are stored on the computer system and other digital devices. It is a known fact that the data we stored on our computer are very important to us. Look at this!!! An important data due for submission to your board of directors, a project report to your management or even something personal as family document could place someone under such attack in dilemma. The ransomware victims are likely to opt into making payment for quick accessibility of their files. "This ransom must often be paid in digital currencies such as Bitcoin. This makes it difficult, if not impossible, to find the culprit. After all, digital coins can be bought and traded anonymously".

1.4 Ransomware: Its Prevention

- Yes, it is not encouraged to make such payments to cyber criminals in order to retrieve your files, but you can't afford to loss your dear data. As your loved ones are so dear to you that you will be willing to make payment to save the lives of your kidnapped loved ones, you will be willing to do anything possible to recover your files, especially when it poses major risk to your business or personal life. To avoid this dare situation, it is important to put proper structure in place that will mitigate against such occurrence. Do you have to make a payment? It is not encouraged for you to make payment to criminals. Paying cyber-criminals makes the business lucrative, and will call for expansion of their horizons. You will also be creating new market for cyber-criminals to carry out further attacks and building their capacity to venture into other types of scheme of attacks in the future. There is no assurance that the criminals will not demand more money from you.

- How do you avoid this dreary situation? The following points could be of help:

- Educate your Employees:

  Employee education on possible attacks of various malwares, including ransomware and how they can have an entry into their system is highly important. Your employees have to

be well informed about phishing mails and how to avoid them. Employees should be aware of the risk involved in clicking attachment from an unknown source, and the vulnerability such actions could introduce into your system. As a system user, you have to beware of unsolicited emails and avoid clicking or downloading unexpected attachments.

- Install genuine Anti-virus Packages:
  Most small organizations are lacking in the actual logic involved in information security. That you are sensitive enough not to have opened scam emails or clicking links that are suspected to be malware or ransomware, are not just adequate. The risk involved is beyond not just clicking, everyone is potentially at risk. However, we cannot assume safety without genuine anti-virus suite which must always be followed with regular updates.

- Have a good Backup plan:
  Constant and regular backup of your files is essential to real safety from ransomware. In fact, that you have a backup is not just enough, but ensuring an efficient offsite backup is very important to any business. Keeping your backup files in the same location as where you operate from, could be very dangerous as such files could be held hostage by a ransomware. You can opt for cloud storage and ensure you make regular back up files to the cloud. Doing regular backup makes it easier for you to retrieve your files in the case of a ransomware attack without recourse to paying a ransom.

1.5 References

- The Oxford Advanced Learners Dictionary
- Erik(2015): Ransomware: a growing threat to the Netherlands
- https://www.dearbytes.com/en/blog/ransomware-groeiende-dreiging-voor-nederland/
- http://www.trendmicro.com/vinfo/us/security/definition/Ransomware

Virtual Currency: Real Security Concerns

By
Adefemi Onanuga,
CISO, Jaiz Bank Plc.

Adefemi Onanuga, is the CISO for Jaiz Bank. With years of IS Auditing experience, he is responsible for executing the Banks Information Security strategy by planning, managing and leading Information Security across the Bank. He is a certified auditor and implementer of various management standards and a topic leader in Big data adoption.

Money remains the ultimate store of value, means of exchange and the barometer for measuring wealth since the gold standard era ended. Money is simply an agreement to use an object e.g. paper, coins, and notes as a means of exchange. In recent times, due to technological advancement, we find ourselves in a hyper-connected digital world where convenience is a key determinant for engaging in business and payment for goods and services. This advancement led to the evolution of other means of exchange and the emergence of the subject matter.

In 2014, the European Banking Authority defined virtual currency as "a digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a fiat currency, but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically". The European Central Bank as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a particular virtual community." The most comprehensive definition yet was given by the Financial Action Task Force: "Virtual currency is a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction".

Virtual currency is not alien to us. It would be interesting to note that technically, we have been using virtual currencies since we started Internet banking. Virtual currencies are fully digitized currencies (i.e. an intangible legal tender and that are stored on a network) and are a type of digital currency implying that every virtual currency is digital. It is common for the terms to be used interchangeably, although, they convey different things. The evolution of virtual currencies began in the year 2009, with the likes of Egold and later more advanced cryptocurrencies like Bitcoin, Namecoin, Peercoin, Auroracoin, and Ethereum emerged.

Virtual currencies are electronic in nature. When they are acquired, the buyer does not get a physical bill or coin, instead, the customer receives electronic units that can be treated like other forms of money. Be it as it may, virtual currencies are not government backed or issued, so it is not a legal tender because it is not binding on anyone to accept it as a medium of exchange. Virtual currencies harness the power of tremendous interconnected systems of unidentified,

private PCs around the world, which keep up and upgrade an open record called the "blockchain." (Consumer Financial Protection Bureau, 2014). Virtual currencies have distinct advantages over banks – it is an open source, continuously available, stable, and secured by its clients rather than the government.

In the course of recent years, virtual currencies have been associated with immense investment losses and illicit online trafficking of black market goods leading to government crackdowns. For comparison, the value of virtual currencies as of January 2014 was estimated at $13 billion while the value of U.S. bills and coins in circulation, reached approximately $1.2 trillion. In 2012, a Washington Post article named three companies that employed full-time economists to manage their virtual currencies.

Virtual currencies offer the potential for business convenience and innovation. However, a lot of critical risk issues primarily affecting users call for concern. There is a need to implement consumer protection, anti-fraud and anti-money laundering measures and data protection. In the same vein, there are compliance implications of the use of virtual currencies and the effects on storage and backup affecting IT governance risk and compliance functions.There are also implications for storage and backup of the use of virtual currencies which can be stored online or offline. In practice, users are saving an encrypted file, which can be on a USB or external hard disk or smartphones or the cloud. The main issue here is the security of the currency being stored, How secure is it? Who can gain access to it? And how can the movement be tracked? . In practice, the Confidentiality and Integrity of the stored currency cannot be guaranteed. In 2011, a security breach was experienced by Bitcoin which led to the compromise of hundreds of accounts and theft of approximately $500,000 worth of virtual money. Since then, the confidence of the general public in the security has been in doubt.

The 2013, New Payment Products and Services (NPPS) Guidance (FATF, 2013) suggested a conceptual framework for understanding and addressing the anti-money laundering / countering the financing of terrorism (AML/CFT) risks associated with one kind of internet-based payment system: virtual currencies. Two narratives emerged:

- Virtual currencies are the wave of the future for payment systems; and
- Virtual currencies provide a powerful new tool for criminals, terrorist financiers, and other sanctions evaders, to move and store illicit funds out of the reach of law enforcement and other authorities.

Consequently, a short term project was initiated with the following objectives:

- Develop a risk-matrix for virtual currencies.
- Promote fuller understanding of the parties involved in convertible virtual currency systems and the way virtual currency can be used to operate payment systems
- Stimulate a discussion on implementing risk-based AML/CFT regulations in this area.

In the nearest future, we might see other forms of virtual currency, possibly, one that converts personal and social data into online currency. It is important for participants in the payment eco-system to raise awareness on the subject matter to match the rate of growth in virtual currencies.

BIBLIOGRAPHY

Virtual Currencies Key Definitions and Potential AML/CFT Risks, Financial Action Task Force (FATF) report, June 2014.

Consumer Financial Protection Bureau, Consumer Advisory | August 2014

https://en.wikipedia.org/wiki/Virtual_currency

https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507

http://bigthink.com/hybrid-reality/future-of-money-classifying-virtual-currency-systems

Shaping the Future of Payments in Nigeria

Visa's vision is to bring more people into the formal banking system through access to electronic banking systems and services to provide Nigerians with a safer, more convenient and reliable way to pay and be paid.

Electronic payments are critical when developing a strong, modern economy. Visa products can promote transparency and accountability, reduce transaction costs and decrease the size of the grey or informal economy, all of which helps to stimulate economic growth and employment.

All evidence points to the fact that the more people who join the banking system, the more stable it becomes. This in turn has a positive and lasting effect on an economy, social reform and government efficiency.

Visa remains committed to finding new ways to enable its client financial institutions to deliver improved services to the banked and unbanked. We continue our support in the markets by extending our products, services and payments expertise; providing extensive financial literacy tools and resources; and developing key partnerships focused on finding new ways to reach the financially underserved.

Benefits of Digital Payments

There are numerous benefits to be derived from card and electronic payments. A growing understanding of these benefits continues to contribute to the growth that we see today in Nigeria and Africa as a whole.

Electronic payments enable access to global products and services, they are more efficient than cash, they promote economic growth, help reduce fraud and allow for people to travel across country borders and transact across the globe safely and securely.

Partnerships with Government

Visa has always advocated for the digitization of payments as that allows Public Agencies and Governments to efficiently configure their workflow processes and electronic document management systems. While some barriers to adoption are rooted in misperception—many features of electronic payments suggest they are safer than other more traditional forms of payment, (like) such as cash.

Implementing appropriate data security standards is particularly challenging, but necessary for electronic payments and mobile money programs. The practice of attempting to “retrofit” existing security solutions and standards such as PCI-DSS to new technologies may have the unintended effect of stifling innovation and preventing solutions from reaching scale. A risk-

based approach to data security allows regulators to adhere to best practices to ensure that sensitive data is protected wherever it is transmitted, processed, or stored while also considering if proposed requirements are appropriate for the programs they are intended to protect.

In Nigeria, Visa has partnered with the government in various ways:

- Visa was instrumental in setting up the Nigeria electronic Fraud Forum (NeFF) in 2012, a body formed to enable information exchange and knowledge sharing on fraud issues amongst key stakeholders, with the objective of ensuring a collaborative and proactive approach to tackling/mitigating fraud and limiting occurrences and losses. NeFF also serves as an official body to represent the industry's position on fraud related issues, while proffering solutions that restore public confidence on card usage and electronic payments in general.

- Last year, 2015, Visa partnered with law enforcement by training the Special Fraud Unit of the Nigerian police force at their invitation by providing a comprehensive insight into card payment fraud, the various fraud *types*, how and by whom the fraud is perpetrated, (individuals, local syndicates or international organized crime organizations), the beneficiaries of fraud proceeds etc. The training also covered police investigation techniques, court room testimony and ended with an in depth discussion into sustainable prosecutions.

Innovation in the Payments Space

Great leaps in the development of personal technology are changing the way the payments industry approaches consumers. Visa's innovations are a reflection of this fast-paced transformation and our goal is to utilize these developments to further drive cash-less societies.

Displacing cash remains the single biggest opportunity for electronic payments in this region.

With the age of increased mobility shaping the payments industry, Visa outlined its view of mobile payments innovation with the introduction of Visa payWave and the regional roll-outs of Visa Checkout and mVisa into a number of markets in Africa.

Another example of enhanced security enabled by innovation is Visa's Mobile Location Confirmation service, available globally. Visa has access to new types of information that build on risk models and help refine precision in analytics.

This service enables a 'match' between the locations of a consumer's mobile device to the location of a Visa transaction. If those locations match, there is greater certainty that the transaction is legitimate. This will drastically reduce incidence of issuers declining transactions purely on the basis of 'suspicion' thus inconveniencing their customers while on travel.

Device identification also powered by innovation tracks if a transaction is being made using a device that the consumer has used before or an unfamiliar device or even an unfamiliar location. This type of data tracking is also adopted by Apple Pay, to ensure that information stolen from a consumer's iPhone cannot then be used on another iPhone without verification or follow up.

Device identification is becoming especially important with the adoption of new payment methods such as mobile. This data will greatly enhance issuers' decision-making ability to identify potential fraud and prompt for verification only when necessary, thus achieving better security and fewer false/positive declines.

In countries where mobile payments rely on established mechanisms such as credit, debit and prepaid cards, data devaluation strategies such as tokenization and end-to-end encryption have been identified as crucial pieces in a strong mobile payments security framework. For example, tokens are unique identifiers that mask Personal Account Numbers (PANs). They can be preloaded onto mobile devices to simplify the role of the digital wallet and eliminate the need for personal information to be stored on merchant servers. Data devaluation could contribute to the security of the mobile payment environment, and may eventually factor into low-value mobile money programs.

To enhance this innovation journey, Visa will open the Dubai Innovation Center in the first quarter of 2016, which will provide clients and partners an innovative space to jointly develop the new commerce applications for the region.

PROMOTING INCLUSION, ACCESS, AND SECURITY

Visa continually develops solutions that support financial inclusion in emerging and developing markets, while also providing the stability and security of Visa's existing networks, expertise, and overall brand promise. The following examples are not comprehensive, but highlight Visa's contributions in this space.

In India and Rwanda, Visa has partnered with MNOs, banks, and—in Rwanda's case, the government—to implement interoperable mobile money programs. Visa's services include customer enrollment, transaction processing and authorization, clearing, and settlement. Visa's program (called mVisa in Rwanda) connects unbanked customers to bank-grade financial services through an account linked to their mobile device. Customers can pay utility bills, send funds to family members, top up their mobile minutes, get cash from an agent, and connect to ATMs. mVisa will launch in Kenya soon with launches in other markets within Africa to follow.

In addition to providing reliability and interoperability, Visa's solutions are secure and risk-based.

Visa invests heavily in advanced fraud-fighting technologies and continues to develop and deploy new and innovative programs to mitigate fraud and protect cardholders. Visa's efforts have helped keep global fraud rates steady near historic lows, enabling account holders to use Visa with confidence. In fact, with technological innovations and advances in risk management, global fraud rates have declined by more than two-thirds in the past two decades.

Visa Digital Enablement Program (VDEP)

The Visa Digital Enablement Program (VDEP) is a program that connects financial institutions and technology companies to simplify and accelerate the roll-out of new payment and commerce services. It is designed to simplify how partners access Visa's secure token technology.

The Program provides fast and easy integration for financial institutions and technology companies. It achieves scale quickly by connecting to one another through VDEP, with no need for a complex set of contractual agreements and technology integrations.

- No-cost commercial framework: Financial institutions, merchants and technology companies can drive growth through a simple, scalable commercial construct with no pass-through fees between technology partners and financial institutions.

- Robust security and consumer data protection: VDEP brings together a powerful combination of secure token technology, risk and fraud management services and customer data protections.

- International scale and reach: Available to Visa's 14,500 global financial institution clients, VDEP will offer banks and technology partners Visa's first platform for delivering secure mobile and digital payment services on a truly international scale.

VisaNet

VisaNet processes more electronic card payments globally than other networks. Visa has an enhanced ability to identify fraud on individual accounts and coordinated attacks on multiple accounts across the system, enabling issuers to stop potential fraud at checkout, before it occurs.

- Visa's Advanced Authorization is an industry-leading security technology that analyzes and scores in real-time, every Visa transaction for its fraud potential. Risk scores are based on a global view of fraud and spending patterns across the entire Visa network providing an analysis of fraud trends.

- In less than one second of processing, the Visa network can analyze transactions and provide risk scores accurately. This speed and clarity help issuers prevent fraud from occurring in the first place, rather than just reacting to fraud after it occurs.

- Visa's suite of fraud detection solutions — Visa Advanced Authorization, Visa Strategy Manager, Visa Risk Manager — highlights the value of intelligent authorization capabilities that can effectively reduce all types of fraud from the center of the network with minimal investments by the industry.

- Visa also looks beyond its own system to help ensure secure commerce for all participants in the payments chain by educating merchants, financial institutions and consumers about how to protect themselves from the threat of fraud.

- Visa provides tips on how account holders can help protect themselves from fraud as well as information on the latest scams at http://www.VisaSecuritySense.com/ and Twitter @VisaSecurity

3D-Secure

The 3D-Secure platform that powers Verified by Visa, is an example of the sort of tools that help prevent fraud in the online environment. New enhancements to Verified by Visa, now allow the issuer to prompt for additional validation only for the riskiest transaction, allowing for a streamlined checkout experience.

But fraud prevention is everybody's responsibility. Knowledge is key and educating customers on the basic steps they can take, to protect themselves (or the do's and don'ts) will go a long way to protecting the industry. Some steps to prevent online fraud would include:

- Keep current with your software and virus protection
- Create strong passwords
- Ignore emails from senders you don't know
- Use your pop-up blocker
- Download files only from sites you know

OTHER PROJECTS

Visa continues to delve deep into creating solutions for individual markets. In Ethiopia, we have provided government travel cards for officials traveling abroad. We are now working with the government there to enable real-time card-to-card money transfers on a global scale at a fraction of the [price] cost. Given the sizable Ethiopian diaspora, Visa's cross border solution is a winning proposition. In India, we have partnered with the government to provide National ID cards with a payment facility secured by Visa's unbeatable security standards. To date, more than 700 Million are enrolled in Aadhaar-based cards. The Government plans to utilize UID (Unique ID) platform to disburse over USD 60 Billion subsidy and welfare G2P payments. Visa was thrilled to potentially provide millions of Aadhaar holders with access to financial services and electronic payments for the first time.

There is a real opportunity in providing government services to millions that are excluded from financial services and Visa continues to embrace this opportunity and work with the Nigerian government to provide very real digitized solutions for Nigerians everywhere.

CONCLUSION

Looking towards the future, we look forward to growing and forging new partnerships to bring greater products and programmes to a large number of people in Nigeria.

Electronic payments play a vital role in shaping global commerce and local economies. For consumers, it means convenience and security; for merchants and businesses, it means more business due to higher purchases. For governments: Greater transparency, and countries: Greater economic development. Visa will continue to share our global experience of driving the growth of electronic payments in over 200 countries and territories around the world, with the regulators and other industry stakeholders in Nigeria.

3rd Party Cyber Risk Management
Using Security Ratings to Manage Cyber Risk

By

Mike Odusami MBA (Warwick), CISSP

President/CEO MAXUT Consulting Ltd.

www.maxut.com

Mike Odusami is the President & CEO at MAXUT Consulting, a Cybersecurity solutions provider with offices in Lagos, and Oakland, CA. USA.
Prior to joining MAXUT Consulting, he was a Product Strategy Director at CA Technologies (formerly Computer Associates) at the European HQ in London England and later at their Global HQ in Islandia, NY, where he led product development for multiple successful IT security and IT Service Management products. In his various roles, he consulted for various F500 companies in Europe and in the US on information security and large business transformation projects, driven by technology.

Introduction

A chain is as strong as its weakest link – so the saying goes.

With an expanding business partner ecosystem, banks and financial institutions are ever more dependent on an interconnected and diverse network of services owned and operated by others. These 3rd party services have opened up new business opportunities, expanded the quality of services offered to retail and corporate banking customers and accelerated internal processes required to meet the faster demands of today's competitive banking environment. Services offered by domestic and international partners, payment platforms managed by others, outsourcing services, cloud technology and telecommunications services provided by 3rd party vendors have helped reshape the banking landscape and brought new levels of business agility to the financial services sector. The rise of Fintech is expected to further expand the universe of core services performed for traditional banking institutions by relatively tech-savvy smaller and younger business partners.

However, the use of 3rd party vendors who have access to sensitive business data, are directly connected to your corporate network, or provide technology infrastructure that brings with it new challenges since each player in the partner ecosystem, including the banks themselves, face cyber risks exposure that differ markedly and are ever-changing. So is the level of expertise and resources that each participant in the partner value chain is able to invest to mitigate their risks. While the financial services sector is in general, at the forefront of the fight against cyber frauds through advanced internal security systems and established best practices for fraud detection, interconnected business partners, especially smaller organizations generally invest less in information security, have less mature technology processes and have a smaller capacity to detect and manage sophisticated security risks. Recent trends point to the use of these less security savvy 3rd party organizations by attackers as staging points for launching more far-reaching attacks on larger organizations within the banking and retailing sectors.

These threats constitute a clear and present danger to the sectors, and have prompted financial regulators and standards bodies around the world to pay closer attentions to the risks posed to

the banking systems by third party vendors. New regulations, guidelines and existing standards are being updated to reflect a focus on continuous third party cyber risk management, which is now a key oversight requirement for the board of directors and senior executives as part of their overall vendor risk management responsibilities.

Security ratings companies such as BitSight Technologies are emerging to augment existing vendor risk management techniques by providing visibility into the effectiveness of cyber security controls promised by third party business partners, as well as those deployed within the banks. Similar to credit ratings provided by credit agencies for managing financial investment risks, security ratings are offered by independent parties and present a way to objectively assess the security performance of all participants in an interconnected partner ecosystem.

Third-Party Vendor Risks Are Real

As evidenced by the spate of security breaches that occurred in 2014 and 2015 at reputable global organisations, your bank's risk exposure from cyber-attacks hinges not only on your own internal security and compliance efforts, but also on the strength of 3rd parties that you share confidential customer data with, and those that are connected to your information systems. For starters some of the most damaging cyber-attacks reported in the last two years were perpetrated by exploiting weaknesses in 3rd party information systems prior to gaining a foothold on the sought-after target. The Verizon 2015 DBIR reports that in 70% of the cases where the motive for a cyber-attack is known, the primary victim is usually infected in the hopes that the true target will eventually become infected.

In one example the attackers injected a malware (software with malicious intents) into the facility monitoring systems of the target bank's building maintenance services company to gain access to and sniff out weak systems within the bank. Once the malware was in place it was only a matter of time before more potent botnets (software that can be controlled remotely by attackers to carry out specific tasks) were implanted and activated for stealing confidential customer data and corporate information which was sent continuously to a command and control center. Stolen customer information is usually a prelude to other forms of malicious attacks (such as phishing attacks via email) and financial frauds including account takeover, and credit cards frauds.

These attacks highlight the shortcomings of current techniques for managing third-party vendor risks, even when the target organizations meet other security compliance requirements such as PCI-DSS. Starting with periodic vulnerability scans and manual vendor assessments which are based on subjective 'point in time' questionnaire responses and a checklist of available security controls at the time the vendor is recruited. The assessments are designed mostly to validate the existence of required security controls by vendors, but they do not verify the effectiveness of those controls on an ongoing basis. Periodic scans provide a point in time

snapshot of known vulnerabilities. Without continuous monitoring backed by real-life data, it is difficult to know for example, how quickly your vendor responds to new threats and vulnerabilities; or how many days a botnet spends on the vendor's network, sending data to attackers before it is discovered and eliminated. And with a typical bank having 200 or more tier one business partners in their 'supply chain', vendor risk management systems based on manual processes are not scalable beyond a handful of vendors (some organizations use Excel Spreadsheets for vendor management, while others with more mature vendor risk management processes use Governance Risk & Compliance (GRC) solutions to help with automated collection of assessments).

The rising concerns about cyber risks to financial institutions through 3rd party vendors coupled with the gaps in existing assessment methods in a constantly changing threat landscape have resulted in regulators around the world, including the Central Bank of Nigeria, issuing new guidance for managing broader cybersecurity risks and those risks specific to business partners.

In the US for example, various financial services regulatory agencies are taking a second look beyond the current system of questionnaires for third party risk assessments and demanding deeper oversights based on continuous monitoring. As an example, the New York State Department of Financial Services (which oversees many of the largest US financial institutions), called for greater cybersecurity oversight by financial institutions and required implementation of policies and procedures by the banks with these minimum requirements:

a) Setting overall cybersecurity policies and procedures;
b) Creating policies for managing third-party service providers' cybersecurity;
c) Hiring qualified CISOs;
d) Hiring qualified staff and vendors to ensure sufficient cybersecurity and cyber-intelligence capabilities;
e) Ensuring CISOs enforce cybersecurity procedures and standards that ensure application security;
f) Employing multi-factor authentication for customers accessing online banking, and for employees and service providers accessing internal systems and data;
g) Auditing all related processes;
h) Maintaining cyber-incident and breach notification policies.

Some of these requirements, or their equivalents, may have been implemented by banks in Nigeria as part of their overall security posture while others such as Item 6, the use of multi-factor authentication for access to banking processes and systems, have been mandated by the Central Bank of Nigeria (see CBN Circular BPS/DIR/GEN/CIR/06/001 dated January 19, 2015).

In addition to implementing the processes and solutions required to meet new vendor risk management guidelines, and to comply with revised standards such as PCI-DSS, financial

institutions are also being asked for information about their firm's exposure to cyber risks by their boards of directors who read headlines about breaches involving high profile retailers and major banks. They are concerned about the financial impact, sanctions by regulators and reputational damage to their brand and their firm's preparedness.

From the foregoing, a combination of demands is driving new approaches to 3rd party vendor and cyber risk management strategies:

- Communication of security information to the board of directors on a regular basis to address their concerns about the cyber risk faced by the banks and demonstrate preparedness
- Managing the security performance of critical vendors and partners with verifiable data minimal overhead, and with automated monitoring
- Meeting regulatory and compliance requirements for continuous monitoring of 3rd party vendors to augment other point in time assessment and audit techniques

Security ratings such as those offered by BitSight Technologies are emerging as one of the popular approaches used for continuous monitoring of vendors to support these risk management strategies. Ratings are quantitative and objective measurements of the security performance of a vendor based strictly on measurements taken from outside the organization. No information is needed from the vendor to create a security rating.

Using Security Ratings to Continuously Manage Vendor Risk and Beyond

Compared to financial investment risks which are usually 'easier' to quantify using tried and tested financial instruments such as credit ratings and risk management techniques, cyber risks are much trickier to assess due to lack of quantifiable methods to rate and determine how secure an organization is compared to others – until security ratings services became commercially available about 4 years ago. The analogy with credit ratings is instructive. Credit scores are generally accepted external indications of the financial health of an individual, corporation or nation state, and have been successful due to their simplicity, accuracy and ability to compare the score of one entity with others. Additionally, the ratings are performed by independent credit ratings agencies, which are autonomous of the credit issuers and investors to remove bias in ratings.

Security Ratings services aim to achieve similar universal acceptance as a standard by providing an indication of the effectiveness of an organization's information security controls based strictly on externally observable metrics tracked by independent parties. To be clear, the ratings are designed to complement other security and compliance programs or tools deployed to safeguard a company's security such as firewalls, intrusion detection/detection systems, two-factor authentication, assessments and audits etc. However unlike manual assessments or periodic vulnerability scans, security ratings are based on continuous measurements.

In one implementation, three categories of metrics are tracked – metrics based on external security events; the organization's security hygiene or diligence; and user behaviour.

Proprietary algorithms and Big Data techniques are then applied to the collected data to create a rating, ranging between a low of 250 and a high of 900 for the organization. This is exceptionally easy to communicate to regulators and internal stakeholders within a bank and to the board of directors.

External events observed include information on active malware, breaches, botnet activities, mass email propagation and other evidence of compromise. Security hygiene is derived from security configuration metrics that are representative of the diligence of the IT team in mitigating cyber risks. A properly configured email server, for example, can help prevent phishing attacks. Other examples of hygiene metrics observed include SSL certificates, use of non-compliant encryption protocols, Open Ports, DNS and DKIM records and others. User behaviour includes activity such as peer-to-peer file sharing.

With these benefits, security ratings are becoming an effective tool for mitigating third party cyber risks, from the onboarding process through continued assessments. Companies have successfully utilized Security Ratings as a tool to screen new vendors and negotiate minimum standards of cyber security performance into contractual agreements. Once onboarded, these ratings can also prioritize actions for further assessments, allowing businesses to focus resources on the highest risk third parties.

Since they were introduced to US and European financial organizations about 4 years ago, security ratings services have found many applications beyond vendor risk management and vendor selection purposes. They have been used by banking customers to support business oversight responsibilities by the board and senior banking executives, including, to evaluate target firms in merger and acquisition due diligence. In a case study with a Bank client that acquired a smaller bank, we noticed a considerable drop in their security ratings score following the integration of information systems from both banks. This was as a result of laxer security diligence by the acquired bank, that showed increased staff use of peer to peer file-sharing sites for media and software downloads, elevated botnets activities and other observed risk vectors which lowered the bank's overall score.

Clients have also used their own security ratings for internal decision-making purposes such as justification for new cybersecurity investments, for demonstrating security performance trends to quantify improvements over time, and for comparisons with other banks. We have also recently seen the use of security ratings in the emerging market for cyber insurance as regulators demand adequate financial coverage for potential losses and legal costs resulting from cyber-attacks. Insurance firms are increasingly relying on security ratings to determine if a client has adequate security controls in place to be insured, and they are continuously monitoring the security ratings.

Payment Systems Security –

A paper presented to NeFF for Annual Report by Skye Bank

Introduction

Electronic payment systems refer to the automated processes of exchanging monetary value among parties in business transactions and transmitting this value over the information and communication technology (ICT) networks. The common e-Payment channels include the payment cards (debit or credit), online web portals, point of sales (POS) terminals, automated teller machines (ATM), mobile phones, automated clearing house (ACH), direct debit/deposit and real time gross settlement (RTGS) system.

Nigeria has remained the fastest growing mobile phone country in Africa and the third in the world where over 60% of the populace are connected (Akwaja, 2010). Thus, Nigeria has great potential for mobile commerce implementation besides the electronic commerce that is gradually gaining momentum. The major distinction between the electronic and mobile business transaction prefixed as “e” and “m” is that the electronic medium offers “anytime access”, while mobile medium offers “anytime and anywhere access” to business processes respectively. However, the success of e-Payment will impact greatly on m-Payment if security and usability issues are well considered. When it comes to credit and debit card payments, several entities are required to process a transaction from start to finish: consumers and their payment cards, merchants and their point-of-sale (POS) payment devices, the card brands (i.e. Visa, MasterCard, Verve etc), issuing banks, and card processors. Enormous amounts of electronic data and digital currency flow through this payment ecosystem as billions of transactions are processed each year.

With access to the sensitive information that enables the exchange of billions of naira in transactions each year, the payments infrastructure is a red-hot target for hackers. The electronic commerce industry has never before been at a more critical juncture in the fight against cybercrime than now. It is the good guys against the bad guys, and the good guys are determined to win. It is no secret the payments ecosystem is vulnerable. Much like the Internet, the payments infrastructure was developed for connectivity, not for security. Now, in the face of serious threats and too many successful instances of hackers exploiting the vulnerabilities of the system, the industry is playing catch up to safeguard it.

Classification of E-Payment

E-Payment is classified into:

1. Online credit card payment system
2. Electronic cheque system
3. Electronic cash system, and
4. Smart card-based electronic payment system.

Fraud and security weaknesses in payments can have an indirect cost as well if they cause concerned consumers and businesses to choose less efficient forms of payment. More broadly, the public's loss of confidence in payments has had significant negative economic consequences in the past. A constant stream of news reports on data breaches, phishing attacks, spoofed websites, payment card skimmers, fraudulent ATM withdrawals, computer malware, and infiltrated retail point-of-sale systems should concern policymakers because it indicates weak payment security and undermines confidence in payments.

Consequently, public and private institutions have evolved a “control structure” to ensure payment security and deter fraud. The control structure takes a variety of forms, such as setting rules that allocate losses resulting from payment fraud, regulating and supervising the activities of some payment participants, designing operational procedures that embed security protocols, and coordinating security efforts. Policymakers must assess how well a payment system manages fraud risks, given constantly changing threats and complex interdependencies that can cause misaligned incentives. A proper assessment is crucial because improvements to payment security are costly and often in fixed infrastructure that is hard to change.

Challenges/Mitigation/Threat of E-Payment

Regardless of the adopted system, the problems militating against e-Payment as listed by Sumanjeet (2009) generally revolve around:

a) Integrity: to ascertain that transmitted financial information is unchanged in transit.
b) Non-repudiation: to ascertain that all parties have no deniable proof of receipt.
c) Confidentiality: to ascertain that transactions are protected from possible eavesdroppers.
d) Reliability: to ascertain that there is reduced possibility of failure.
e) Authentication: to ascertain that there are reliable proofs of identities of all parties involved.
f) Authorization: to ascertain that individuals are recognized and granted the desired rights and privileges.

Therefore, any reliable form of electronic payment should guarantee privacy, integrity, compatibility, efficiency, acceptability, convenience, mobility, anonymity and low financial risk.

Changes in Methods of Fraud and Attack

Some methods of committing payment fraud are used consistently while others have changed in recent years. Access to sensitive data has become a key factor enabling many methods of payment fraud. Stolen data allow fraudsters to misrepresent authority, counterfeit cards and cheques, and take over or create new payment accounts. Data are more valuable to fraudsters because today, payers use fewer paper cheques and more electronic payments (cards, ACH), thus initiating more non-cash retail (smaller-value) payments with data alone.

IDENTITY THEFT/SOCIAL ENGINEERING: One of the greatest threats to e-Banking is the increasing trends of identity theft, which is a major challenge to the Internet age (Helmbrecht, 2008). Therefore, there is need for a technology that is safe, convenient and not too demanding on the part of the user, because of the level of literacy in the developing nations of the world, particularly Nigeria. All the banks have one form of e-Payment system or the other. Alao (2009) reported the colossal amount of money lost in Nigeria to ATM fraud through ATM card cloning, PIN theft among others, and government had resorted to removing ATM from public places as well as installing security cameras at the ATM locations to track the activities of fraudsters. However, the level of ICT usage notwithstanding, the level of adoption of e-Banking by the citizen is still very low. Although card cloning fraud has been eliminated with the introduction of chip and pin cards, the increasing use of social engineering tactics by fraudsters on unsuspecting card holders is a source of concern.

UNENCRYPTED DATA: Typically, when a consumer swipes his or her credit or debit card at a merchant location to make a purchase, cardholder data is in the clear text as it leaves a merchant's terminal and is not protected until it is either tokenized in a gateway, or encrypted at rest in the processing platform's data warehouse. This is a fundamentally flawed security model that puts cardholder data at risk of being compromised should it get in the hands of cybercriminals who use methods like network or memory sniffer malware and RAM scrapers. This puts the entire payments ecosystem in jeopardy. In the case of a successful data breach, merchants face the devastating financial and reputational repercussions of the compromise, and consumers may be forced to deal with the consequences of credit card fraud.

SOFTWARE TECHNOLOGY: While technology solutions are paramount to safeguarding the payments ecosystem, an unscrupulous user obtains a user account information from prospective user and improperly initiates an unauthorized payment in e-commerce transactions where the card is not present. Fraudsters also obtain raw payment cards and manufacture counterfeits with data stolen via card skimmers fit onto an ATM, sometimes also with a remote camera installed to capture the cardholder's PIN. Computer viruses infect personal computers with key loggers that harvest online banking credentials, which are then used to generate fraudulent wire, cheques, or payments.

THIRD PARTY **FRAUD:** One goal of strong payment security is to prevent third-party fraud—payment fraud perpetrated by individuals other than the legitimate account holder. Successful third-party fraud occurs when payment initiation (creating a payment order), authentication (confirming a payer's identity), or approval (screening the payment order for suspicious characteristics before granting approval) fail to prevent an unauthorized transaction. All payment participants have a role in preventing third-party fraud. In a cheque payment, for example, the account holder should ensure the cheque book is in the hands of authorized payers, the payer should verify the signature on the cheque and ensure that it is not a counterfeit cheque.

DEFENDING THE PAYMENT SYSTEM TO PREVENT FRAUD

Incentives for payment participants to secure the payment system are often misaligned and have led to inadequate security. Payment networks establish specific controls to ensure security and to limit fraud. Public authorities pass laws, write regulations, and monitor payment system participants for compliance. These activities form a "control structure" that determines how a payments system manages risks into protecting privacy and integrity, and how dissimilar conditions might lead to different defensive strategies.

DATA ENCRYPTION: To ensure the integrity of an electronic check file, some financial institutions and processors encrypt the file when transmitted. However, there is no legal or regulatory requirement to encrypt transmitted electronic check files, nor are there common standards of encryption to follow. Some financial institutions and processors agree bilaterally to transmit encrypted files. The practice could become more widespread, however, if standards for check file encryption were established. For a secure online payment system, the transaction flow must be secured with end-to-end encryption. In today's day and age, there is no such thing as safe software. Data need to be protected at all points, end-to-end, from the moment the transaction is initiated and through the processing network to truly be effective. Secure online payment system requires end-to-end encryption. The online payment ecosystem is a prime target for cybercriminals.

SECOND FACTOR AUTHENTICATION: This is where hardware enters the equation. By using a hardware-protected tamper-resistant security module (TRSM), data is protected at the moment of swipe, before it enters the merchant system, beefing up security during a critical leg of the transaction lifecycle. It is this intersection of strong end-to-end encryption security software, tamper-resistant hardware and tokenization, which replaces cards' 16-digit payment account numbers with token values that provides merchants optimal protection. By adequately protecting and removing the data that the criminals are after, merchants are essentially removing from the hackers' cross hairs.

COMMON STANDARD: Standardization improves efficiency because processors adapt their systems to a limited set of protocols. At times, however, private providers can rapidly introduce security solutions before standardized solutions are developed and adopted. A second long-run principle places emphasis on compliance with security standards over the speed of their development. While proprietary standards may be quick to develop, an inclusive and cooperative development process, such as that provided by PCIDSS, improves motivation to comply with standards. In any large and diverse payment system, even well-designed security standards will be adopted unevenly across participants, so it is critical to motivate participants to comply. Some delay in developing security standards may be valuable overall, if more payment participants adhere to the standards.

INCENTIVES: Incentives are crucial to encourage good security practices among all payment participants. (E.g. cheque payments, statutory law sets the basic rules to allocate liability for fraud losses). The rules use a basic principle that the entity is in the best position to deter cheque fraud and will bear the losses for a cheque it processes. Applying the same principle to data could help protect sensitive data on home computers. Malware, such as key loggers installed on desktop computers, gives fraudsters login credentials of consumer or business payment accounts. Stolen credentials allow unauthorized access to online banking systems and thus, the ability to initiate fraudulent payments. Devising systems to prevent malware is a challenge because many users are unable to protect their computers. Financial institutions often refuse to provide security advice or anti-virus software because they may bear liability if their customers' computers become infected. A better control point is the Internet Service Provider (ISP). ISPs have the ability to monitor their users' Internet traffic to detect malware infections, because responsibility for malware is unclear, ISPs resist regulatory requirements to detect and clean up infected computers. An alternative is to make ISPs legally responsible for the damage caused by infected computers on their network, but at the same time provide incentives and compensation if the ISPs assist customers in securing their computers. Improving the security of home computers could reduce fraud on all forms of payments. The key is to provide the correct incentives to effectively control security risks. Implementation requires changing laws concerning liability over damage due to malware and creating institutions to coordinate efforts to prevent and remediate malware.

AUTHENTICATION AND AUTHORIZATION: Financial institutions have known for some time that usernames and passwords alone are insufficient to effectively protect user accounts. Numerous strong authentication techniques are available to address a wide range of threats that are still relevant, involving the user in some additional authenticating steps, at login time, transaction execution time, or both. Amplifying the out-of-band one time passcode method, the user is not only sent a one-time passcode via out-of-band communication (e.g., SMS or voice channel), but is also sent a summary of the transaction that is about to occur; for example: “Wire transfer N15,325 from acct 132382 to 482763. Confirmation code 193713”; user can then review the details, and only proceed in their browser if they recognize the details.

Conclusion

The level of adoption of ICT in the banking sector in Nigeria is on the increase, while the amount of cash in circulation is equally increasing, a situation which is attributable to lack of safety, security, privacy and reliability in the e-Payment instruments. Therefore, the introduction of ATM with biometric authentication will ameliorate these challenges as it will enhance safety, security, and privacy. Furthermore, the fingerprint authentication will be a cheaper alternative than to relocate all ATMs in Nigeria (several thousands of them), to safer premises and the inclusion of security camera at each location.

The payment industry is working hard to protect payment data, improve security, and prevent fraud. The options to improve security discussed in this article, while representing only a subset of possible approaches to strengthen security, involve all elements of the control structure—governance, rules, security technology, and enforcement. Fraudsters are attacking payment systems to obtain sensitive data useful for payment fraud with a vigor unseen in the past. Data security would be enhanced by immediate acceleration of private and public efforts encouraging payment participants to adopt effective security protocols. The payment industry should consider improving elements of the control structure to better protect payments and respond to attacks with initiatives that promote information sharing on security threats. Shared security techniques, protocols, and standards would also help.

Furthermore, the payment industry should provide data measuring progress in payment security as well as weaknesses that require attention. Because of the modern payment system's complexity, policymakers and industry leaders need a broad perspective to judge weaknesses in the control structure over payment security and the control structure's ability to adapt, as new fraud methods arrive. A long-term perspective is especially important because fraudsters' incentives to exploit security weaknesses will not disappear. Critical contributions to the control of payment fraud will continue to come from private security services. Improvement could also come from contributions that take a payment system-wide approach, such as a group coordinating diverse payment participants, promoting cooperation, and finding effective solutions to weak payment security.

REFERENCES

1. Akwaja Chima (2010). “Nigeria Connects 99 million Subscribers”, Fin. Standard., 10: 15-512.
2. Alao Salimon (2009). Need to guard against ATM frauds, Fin. Standard., 9(479): 17-18.
3. Ayo CK (2009). “Information Systems and Technologies”. McKay Educational Series, p. 649.
4. Ayo Charles K., Uyinomen O. Ekong, Fatudimu Ibukun Tolulope, and Adebiyi Ayodele A, (2007): M-Commerce Implementation in Nigeria: Trends and Issues, Journal of Internet Banking and Commerce, August 2007, Vol. 12, No.2, Available at: http://www.arraydev.com/commerce/JIBC/2007-08/Ayo_final_PDF%20Ready.pdf
5. Okoegwale Emmanuel (2011): “Nigeria Mobile Payment & Agency Banking Risk”, accessed date: May, 2011, available at: http://mobilemoneyafrica.com/?p=3422
6. Ojo A. T. (2004): “Enhancing the efficiency of the payment system: Conceptual Framework”, A paper presented at the 9th CBN Monetary Policy Forum, Abuja, May 2004.
7. Abrazhevich, D. (2002) „Diary on Internet Payment Systems', Proceedings of the British Conference on Human Computer Interaction, London, England.

8. Akinyede, R. O. and Afolayan, O. J.: Electronic payment system revolution in Nigeria banking industry, in proceedings of the 20th Annual National Conference of the Nigeria Computer Society, vol. 17, pp. 107-115, (2006).
9. American Bankers Association. 2013. “2012 Deposit Account Fraud Survey Report.”. 2011. “2010 Deposit Account Fraud Survey Report.”
10. Anti-Phishing Working Group. 2014. “Phishing Activities Trends Report,” available at http://docs.apwg.org/reports/apwg_trends_report_q1_2014.pdf.
11. Association for Financial Professionals. 2014. “Payments Fraud and Control Survey.” April.
12. Baddeley M (2004). Using e-Cash in the new Economy: An Economic Conceptual Framework”, A paper presented at the 9th CBN Monetary Policy Forum, Abuja, May.

Ransomware – A Growing Threat

By
Adeolu A Adebisi
B.Sc. (Comp. Science), MTECH (BIS), CISA, CISM, CISSP
Head, Information Systems Audit (Internal Audit Group)
Skye Bank Nigeria Plc.
aadebisi4@skyebankng.com

1.0 Introduction

Ransomware is a computer hostage, lockdown and hijacking menace similar to human kidnapping where a ransom is being demanded before the computer is released for use. Ransomware is one of the most lucrative and broad-reaching campaigns being witnessed by Internet users today. This hostage focuses on the victim's files database and other important applications residing on the computer. The hostage is a form of malware attack in which rogue software code effectively holds a user's computer hostage until a "ransom" fee is paid. In the recent time, this attack according to Paul (2015), on the existence of the ransomware, it was confirmed that ransomware, in various forms, has been around for more than a decade. The past three years have seen a steep rise in incidents involving the programs, which often infect users via malicious e-mail attachments or drive by downloads from compromised websites or malicious web advertisement.

2.0 Brief background on Ransomware.

The evolution of ransomware dated back to 1989 with advances in technology and challenges facing the economy, security, and culture. The attack is not severe in developing nations and less integrated hi-tech, but very high and rapid in developed and highly integrated/hi-tech environment. Kevin et.al (2015) pointed out that ransomware has evolved considerably since the origin and appearance of the AIDS Trojan released into the unsuspecting world through snail mail using 5¼" floppy disks in 1989. It was however, re-affirmed that the AIDS Trojan was ultimately unsuccessful due to a number of factors. Some of the factors are, few people used personal computers, the World Wide Web was just an idea then but not fully accepted into businesses and the internet was mostly used by experts in the field of Science and Technology, Kevin et.al (2015).

It is worthy of note and mention that computers and devices not connected to an internet or super highway information (World Wide Web) are mostly free from ransomware attacks.

3.0 Types of Ransomware

There are two major forms of Ransomware. It comes in the form of both hardware and software and the attack is to completely lock down either hardware or Software involved. Hardware type is simply called locker ransomware (Computer locker).

Locker Ransomware: This is a form of ransomware that denies individual access to the computer or device. Locker ransomware is designed to deny access to computing resources.

This typically takes the form of locking the computer's or device's user interface and then asking the user to pay a fee in order to restore access to it. However, locked computers will be left with limited capabilities, such as only allowing the user to interact with the ransomware and pay the ransom. Most often, access to the mouse might be disabled and the keyboard functionality might be limited to numeric keys, allowing the victim to only type numbers to indicate the payment code.

Software type, Crypto Ransomware: This on the other hand, is the type of ransomware designed to find and encrypt valuable data stored on the computer, making the data useless, unless the user obtains the decryption key after the ransom has been paid. These categories of ransomware discussed will be of no use, and the impact on the hardware and software will be limited without the agents of propagation.

3.1 Agents of Ransomware: The propagation of ransomware is made possible through the following agents which are common malware distribution services that are running like any other business service on our computers and networks. Amongst these malwares are:

- Spam email: - The spam usually comes in the form of an email containing a malicious attachment or a link in the email leading to a site hosting an exploit kit. The spam may also involve the download of malware through other social-engineering means;
- Downloaders & botnets: - This method is one of a number of ways to distribute malware known as downloaders. Once the downloader infects a computer, its job is to download secondary malware onto the compromised system. The cybercriminals behind downloaders offer a malware-installation service onto already compromised computers, at a price to other malware authors.
- Social engineering and self-propagation:- This is an attack against people as a way of getting access to targeted systems and potentially an effective way for the ransomware to spread itself. Ransomware is continuously spreading through a network, infecting multiple computers and demanding payment each time, the cybercriminal's promise to repair the damage, after the victim pays the ransom is broken. With all these techniques and methods, attackers always know and have their targets.

4.0 Main Target of the Attackers.

The ransomware attackers focus on the Home users, Businesses and Agencies. The home users form the larger part of the target and the most affected are the individuals who are not fluent, savvy with computers or are not familiar with Ransomware, how it works and least access to technical assistance. This sometimes leave them helpless & isolated and put them under the pressure to pay. For many businesses, information and the technology is their life

blood, without which the act of conducting day-to-day business is impossible. Computers used for businesses are also more likely to contain sensitive data and documents of critical importance, such as customer databases, business plans, proposals, reports, source code, forms, and tax compliance documents. The loss of this information could have a catastrophic impact on the business. In addition, agencies such as educational institutions, non-governmental organisations, health departments, government offices, and even law enforcement agencies are not excluded from the attention of these cybercriminals. In most cases, these agencies are the main target because of large fund always budgeted or assigned to run them.

The spread of these attacks is on the alarming rate. Nearly 1 million new malware threats including a variety of hostile software such as viruses, spyware, trojan horses and malicious programs were released every day, this was according to the Holly's report, which analyzed emerging trends in attacks, malicious code activity, phishing and spam. Meanwhile, ransomware attacks, which restrict access to the computer systems they infect, increased by 113%, driven by an over 4,000% increase in crypto-ransomware attacks. Victims are offered a key to decrypt their files, but only after paying a ransom that can range from $300-$500—and there is no guarantee that their files will be unlocked. It is also noted that, the mining industry, which includes oil & gas, was the most-targeted sector globally in 2014. Other high risk targets were the manufacturing, transportation and communication industries. The effective decision to take by a victim after the attack becomes so difficult- paying ransom to hidden person and to whose account?. The threat, also comes with a deadline if the ransom is not paid within the given period. On the final note, the attacked victim is always at a loss if the money is not paid.

5.0 Victim's Position (Pay or not to Pay).

As the world is moving towards globalization through internet, many other devices apart from personal computers, such as smartwatch, a smart TV, a smart fridge, a smart lock, an internet-enabled car, smart city, were not spared from these attacks. Chances are, that we could be prone to cyber-attacks or malwares in one way or the other, because of changes in our daily lifestyle. What is the way forward? If your computer gets hacked and infected with malware that holds your data for ransom, just pay off the criminals so you can have the chance to see your valuable data again. If you happen to miss the deadline, the virus will uninstall itself and the files cannot be decrypted; meaning, both the attackers and the individual or the organization is at a loss. Sometimes, the criminals say that they will unlock the information and /or data if the victim pays the ransom and that does not actually mean they will. In addition, though they may unlock the data that has been encrypted, that does not mean the computer is safe and sound because a path had been established. The computer may still be infected with the same malware that enabled the ransomware again and again, for further threat. Furthermore, the more often people pay ransom, the more profitable (and popular) this nasty form of malware becomes. At this point, it is better to stay safe than to have encounter with this ransomware. Once this attack comes, there may sometimes be no way out of it than to pay the ransom. It is however,

important to note that prevention is better than paying the ransom. There are some preventive measures that will be mentioned and discussed in the next section. Adherence to them would be of help to guide and prevent individuals, businesses and agencies from falling into the trap.

6.0 Prevention and Guides against Ransomware.

The security report on the website of Zone Alarm highlighted the following guides that an individual, organization and agencies can practice, that can serve as best defense for the ransomware:

- Never open attachments or embedded links in emails unless you know with 100% certainty that they are safe.
- Run a top-notch antivirus that catches dangerous links before they make it into your inbox.
- Do not click on a link or attachment in an email unless you are positive that it is from a trusted source.
- If the email looks slightly suspicious to you, that is because it is probably suspicious.
- When files have a double-extension such as txt.vb or jpg.exe, be careful! Windows will often hide common file extensions as a default setting; such as Paint.exe appearing as Paint. Double extensions exploit this by hiding the second, dangerous extension and making you feel secure with the first extension. If a common file type's extension suddenly becomes visible, right click on it, select Properties, and find the complete file name.
- If you are using an email retrieving program, such as Outlook, disable the image previews! Many email services like Outlook or Thunderbird tend to load attachments automatically for convenience.
- Be careful with unusual emails received from random companies. If you receive an email from a company that's trusted, but it requests information or suggests a file to run, log into your account on that company's page and look for notifications there. Scammers know which companies you trust, and they will copy the businesses' email style to catch you off guard.
- Be cautious with USB drives! When you plug someone else's USB drive into your computer, you are risking the spread of infection via the drive itself, not the file you are attempting to share. Always transfer files between computers using emails.
- Install a powerful pop-up blocker as many pop-ups can also contain dangerous links.
- Keep all your programs up to date. Nothing invites malicious programs more than software that is outdated. The chances of getting hit by ransomware, or any malware in truth, decrease significantly when software is running at its most current version.
- Stick to safe websites and you will eliminate a venue through which hackers try to get into your PC: through malicious scripts.
- Back up your files, all of them, almost daily, weekly and monthly. If you do get hit by ransomware, you may just have to say good-bye to the data that has been encrypted.

One can format the whole system and restore new data and information from the backup rather than paying the ransom. That is why it is so important to make sure that back up of all files are up to date.

6.0 Conclusion

Ransomware is like any other attack in computing environments. It has come a long way back when programmers and developers tried to brag about writing a powerful and sensitive programs that can disturb other computers, applications and networks environment. Then, there was no monetary value attached, but ego. It was less than two decades ago when countries started experiencing the explosion of the internet, economic meltdown and culture distortion that ransomware became rampant. It is here to stay I assume, and that is why the good guys are doing everything they can to stop it, the bad guys are doing everything they can to make it even more sinister. No person, organization and agencies need to be a victim, though. Taking preventative measures and advice is critical, while it may take some time to back up files, update software, and verify unexpected emails before opening the attachments. One thing is clear, none of these minor hassles are as inconvenient and damaging as having your files held ransom by unscrupulous hackers.

Reference:

1. Holly Ellyatt (2015): CyberSecurity; ETGlobal cyber-attacks on big business up 40 percent in 2014.
2. Kevin Savage, Peter Coogan and Hon Lau (2015): SECURITY RESPONSE: The evolution of ransomware. Version 1.0 – August 6, 2015.
3. Paul Roberts (2015): The Security Ledger; Digital Guardian. Access on 23 January 2016. Available online at https://securityledger.com/2015/10/fbis-advice-on-cryptolocker-just-pay-the-ransom/.
4. Zone Alarm (2015): Ransomware – The Nasty Type of Malware That's On the Rise. Access on 24 January 2016. Available online at http://www.zonealarm.com/blog/2015/11/ransomware-real-reprehensible-and-on-the-rise/

NeFF Retreat

NeFF Retreat









RANSOMWARE

By
Digital Encode

INTRODUCTION

1. Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive while some may simply lock the system and display messages intended to coax the user into paying.

2. Ransomware typically propagates as a Trojan like a conventional computer worm, entering a system through, for example, a downloaded file or a vulnerability in a network service. The program will then run a payload that will begin to encrypt personal files on the hard drive. More sophisticated ransomware may hybrid-encrypt the victim's plaintext with a random symmetric key and a fixed public key. The malware author is the only party that knows the needed private decryption key. Some ransomware payloads do not use encryption. In these cases, the payload is simply an application designed to restrict interaction with the system, typically by setting the Windows Shell to itself, or even modifying the master boot record and/or partition table which prevents the operating system from booting at all, until it is repaired.

OPERATION

3. Ransomware payloads utilize elements of scareware to extort money from the system's user. The payload may display notices purportedly issued by companies or law enforcement agencies which falsely claim that the system had been used for illegal activities, or contains illegal content such as pornography and pirated software or media. Some ransomware payloads imitate Windows XP's product activation notices, falsely claiming that their computer's Windows installation is counterfeit, or requires reactivation.

   These tactics coax the user into paying the malware's author to remove the ransomware, either by supplying a program which can decrypt the files, or by sending an unlock code that undoes the changes the payload has made. These payments are often delivered using either a wire transfer, premium-rate text messages, through an online payment voucher service such as Ukash or Paysafecard, or most recently, the digital currency Bitcoin.

CRYPTOLOCKER

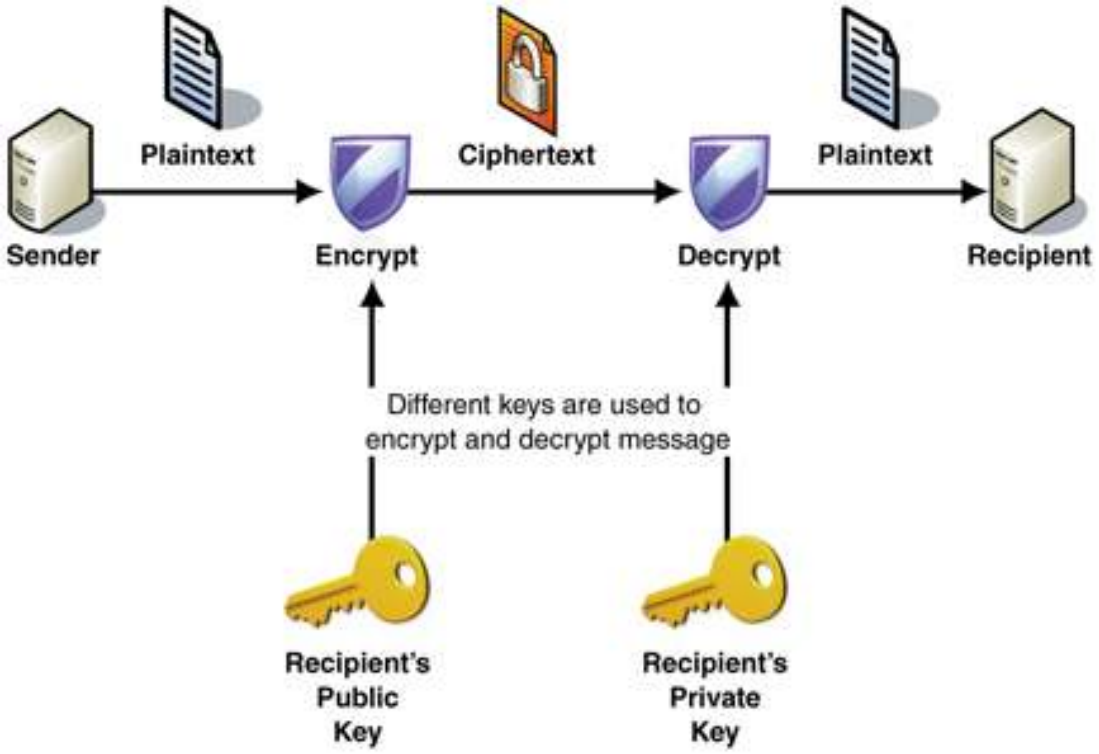
4. Introduction. CryptoLocker is a ransomware which targets computers running Microsoft Windows and was first observed by Dell SecureWorks in September 2013. CryptoLocker is propagated via infected email attachments, and via an existing Botnet. When activated, the malware encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography, with the private key stored only on the malware's control servers. The malware then displays a message which offers to decrypt the data if a payment (through either Bitcoin or a pre-paid cash voucher) is made by a stated deadline, and threatened to delete the private key if the deadline passes. If the deadline is not met, the malware offered to decrypt data via an online service provided by the malware's operators, for a significantly higher price in Bitcoin.

Although CryptoLocker malware can be removed, the files encrypted by malware will remain encrypted, which is considered infeasible to break. Many have said that the ransom should not be paid, but did not offer any way to recover files; others said that paying the ransom was the only way to recover files that had not been backed up.Some victims claimed that paying the ransom did not always lead to the files being decrypted.

1. CryptoLocker generates a 2048-bit RSA key pair uploaded in turn to a command and control server, and used to encrypt files using a list of specific file extensions. The malware threatens to delete the private key if a payment of Bitcoin or a pre-paid cash voucher is not made within 3 days of the infection. Due to the extremely large key size it uses, analysts and those affected by the worm consider CryptoLocker to be extremely difficult to repair. Even after the deadline passes, the private key could still be obtained using an online tool, but the price would increase to 10 BTC which was equivalent to approximately US$2300 as of November 2013.

7. Files targeted are those commonly found on most PCs today; a list of file extensions for targeted files include: 3fr, accdb, ai, arw, bay, cdr, cer, cr2, crt, crw, dbf, dcr, der, dng, doc, docm, docx, dwg, dxf, dxg, eps, erf, indd, jpe, jpg, kdc, mdb, mdf, mef, mrw, nef, nrw, odb, odm, odp, ods, odt, orf, p12, p7b, p7c, pdd, pef, pem, pfx, ppt, pptm, pptx, psd, pst, ptx, r3d, raf, raw, rtf, rw2, rwl, srf, srw, wb2, wpd, wps, xlk, xls, xlsb, xlsm, xlsx.

8. Cryptolocker encrypt users' files using asymmetric encryption, which requires both a public and private key. Below is an image depicting the process of asymmetric encryption.



The public key is used to encrypt and verify data, while private key is used for decryption, each the inverse of the other. The decryption is impossible unless a user has the private key stored on the cybercriminals' server. Infected users also have a time limit to send the payment. If this time elapses, the private key is destroyed, and your files may be lost forever. However, in some cases, it may be possible to recover previous versions of the encrypted files using System Restore or other recovery software used to obtain shadow copies of files.

MITIGATION

The system should be hardened properly and following points are to be configured to avoid the compromising of system by any ransomware like CryptoLocker:-

(a) Adhere to strong password policy with 3 layers of protection.
(b) Create regular backups and restore points.
(c) Patch your system regularly.
(d) Use Antivirus and update it regularly.
(e) Use encryption to store important data.
(f) Take backup of system and important files on different media regularly.

(g) Disable Autorun.
(h) Use firewall, Anti-spyware programs.
(j) Disable Remote sharing (Desktop, Network).
(k) Disable unnecessary services and block unused ports.
(l) Disable Wi-Fi / Bluetooth network when not in use.
(m) Do not use pirated/unauthorized softwares.
(n) Do not use USB mass storage devices.
(o) Do not share your password or use same password for different sites.
(p) Don't give administrative privileges to user accounts.

CONCLUSION

10 There is a constant growth in the security risks among Windows users, be it worms, Trojans or ransomware. In case of systems infected with ransomware, if an attack is suspected or detected in its early stages, it takes some time for encryption to take place, then immediate removal of the malware before it has completed encryption would limit its damage to the data. One of the best way to protect the system from ransomware is by hardening and updating OS and antivirus regularly.

REFERENCES.

11. References are as under :-

(a) en.wikipedia.org/wiki/Cryptolocker
(b) http://www.darkreading.com/attacks-breaches/new-zeus-banking-trojantargets-64-bit-s/240164713
(c) http://blog.fortinet.com/Ransomware/
(d) http://www.symantec.com/connect/blogs/grappling- zero access-botnet
(e) http://threatpost.com/zeus-source-code- leaked-051011
(f) http://www.zdnet.com/cryptolockers-crimewave-a-trail-of-millions-inlaundered-bitcoin-7000024579/
(g) http://threatpost.com/virut-and-waledac-botnets-spamming-sharedmachines 011513/
(h) http://www.fortinet.com/resource_center/whitepapers/quarterly-threatlandscape-report-q213.html
(l) https://www.decryptcryptolocker.com/
(j) http://www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-nationalaction-against-gameover-zeus-botnet-and-cryptolocker-ransomware-chargesbotnet-administrator
(k) http://www.kyrus-tech.com/cryptolocker-decryption-engine/


NeFF

Nigeria electronic Fraud Forum: Strides and Strategies

BY
AJIBOYE BABATUNDE CHUKWUMA
SHARED SERVICES OFFICE AND SECRETARY,
NIGERIA ELECTRONIC FRAUD FORUM

Babatunde is a Manager with the Shared Services Office in the Central Bank of Nigeria. He also doubles as the Secretary of the Nigeria electronic Fraud Forum (NeFF).

1) Introduction:

In order to grow the acceptance of alternative payment channels in a cash endemic society like Nigeria, and build confidence in the usage of these channels, an effective Anti-Fraud policy is imperative. We cannot over-emphasize the harmful effects that fraud has on an economy and to a greater degree, society. Payments System stakeholders are not immune to this reality, and have come together to deal with the menace, taking into cognizance the particular nature and extent it presents itself in our country either as internal or external threats.

Payment System stakeholders in furtherance of the Payment System Transformation initiative that commenced in 2011, and with the imminent takeoff of the then "Cash-less Lagos", it was expected that electronic fraud attempts would increase as we experienced a significant growth in electronic payments. Given the importance of providing secure payment systems, whilst ensuring public confidence in electronic means of payment, the role of proactive fraud management could not be overstressed.

It was within this context, and leveraging on the lessons learnt from past experience (e.g. ATM magnetic stripe card frauds) that the Nigeria electronic Fraud Forum (NeFF) was established.

2) Why an Industry wide Fraud Forum?

i. No one single institution can defeat fraud by itself; a significant exposure exists by operating in isolation

ii. Fraud by its nature affects all institutions, and as such, it is more effective to work as a group. In addition, customers do not perceive fraud as an issue with a specific bank, but with electronic payments overall, which eventually affects the entire industry and not just the institutions that have been impacted by fraud.

iii. An effective Fraud Forum will protect the integrity of the banking industry from criminal threat, as well as boost public confidence in the use of electronic payments

iv. Important stakeholders such as Law Enforcement agencies will be more likely to listen and commit resources to fight crime if they know they are dealing with an industry body who expresses a common opinion and requirement. The same also applies to other stakeholders such as payment service providers, card schemes, telecommunication companies, etc.

v. Criminals will capitalize if there is disunity amongst the banks (as has been experienced in the past, where the same fraudster attacks multiple banks, and is not caught due to lack of information sharing)

vi. Resources, expertise and finance can be shared more effectively by Fraud Forum members to resource fraud reduction projects and effectively target specific issues.

vii. Dealing with the players in the e-payment delivery value chain on risk requirements is made significantly easier because the Fraud Forum can articulate its common requirements.

3) Aims and Objectives of NeFF

The aim of NeFF is to enable information exchange and knowledge sharing on fraud issues amongst key stakeholders, with the objective of ensuring a collaborative and proactive approach to tackling/mitigating fraud and limiting occurrences and losses. In addition, NeFF aims to serve as an official body to represent the industry's position on fraud related issues, while proffering solutions that restore public confidence on card usage and electronic payments in general.

The key objectives of NeFF are as stated below:

Educating and informing all banks and other stakeholders on various electronic fraud issues and trends (both locally and globally)

Proactively sharing fraud data/information amongst banks and service providers, to enable prompt responses to prevent and/or limit fraud losses.

Formulating cohesive and effective fraud and risk management strategies, and defining key requirements as relates to e-payment security on behalf of the industry

4) Delivering on the NeFF mandate – Our Strides

a. Information Exchange and Knowledge Sharing: The Forum has been able to enhance the process and efficiency of learning by the Industry. 16 different presentations have been made on varied topics that are central to e-fraud control in Nigeria.

Date	Theme	Topic	Presenters
March 2012	Electronic Payments: Current and Emerging Fraud Trends	Cashless Nigeria & E-Fraud: A Way Forward	eTranzact
		Fraud Trends and Fraud Management	Interswitch
		Electronic Payments: Current and Emerging Fraud Trends	Unified Payments
April 2012	Cashless Nige ria: Likely frauds on e -payment channels (POS) and how to mitigate them	Fraud as it appears to PTSPs and PTADs	ETOP Nig. Ltd.
			NIBSS
May 2012	Frauds on e -payment channels (Mobile): An Industry Perspective		Citiserve
			Eartholeum Networks
			E-PPAN
			Zenith Bank
June 2012	Cashless Nigeria: Likely frauds on e -payment channels (Web) and how to mitigate them		Interswitch
			Zenith Bank
July 2012	Securing Electronic Payments Infrastructure: The need for standards		Diamond Bank
		Securing Electronic Payments Infrastructure: The Need for Standards	Interswitch
August 2012	e-Payment Fraud Trends	e-Payment Fraud Trends: Interswitch Perspective	Interswitch

Date	Theme	Topic	Presenters
September 2012	Money Laundering with Electronic Payment Systems	Anti-Money Laundering Issues on Emerging E - Payment Platforms	Access Bank
		Anti-Money Laundering Issues on Emerging E - Payment Platforms	First Bank
		Anti-Money Laundering Issues on Emerging E - Payment Platforms	Financial Policy and Regulation Dept. CBN
October 2012	Challenges of Identi ty Management on E - Payments System in Nigeria		CHBO
			Interswitch
			NIBSS
			SystemSpecs
November 2012	Creating awareness and enlightenment on e - payments system fraud and its mitigation		FCMB
			E-PPAN
		Proposed Enlightenment Campaign & Training for Law Enforcement, Legislative & Judicial Personnel	NeFF Sub - Committee
		Controlling Fraudsters Access: Need for Centralized Authentication?	Interswitch
April 2013	"e-Fraud in 2012: Who got hit, Who got caught and Lessons Learnt"		Interswitch
			NIBSS
			Digital Encode

Date	Theme	Topic	Presenters
May 2014	Current Fraud Assessment		Paga
June 2014	The Journey Towards A Cash-Less Nigeria: Strategies to enhance security, reduce spamming and increase sensitization		Digital Encode
			Interswitch
	e-Fraud Consumer Sensitization		E-PPAN
August 2014	Denial of Service Attacks: An emerging National Security Threat		ONSA
	Denial of Service Attacks: Measures To Stem The Tide		Digital Encode
March 2015	Shining a light on insider abuse		NIBSS
	Shining a light on insider abuse		Digital Encode
June 2015	Cybersecurity: The Need For Standards		ONSA
			Digital Encode
			Digital Jewels
August 2015	Cybercrime Prohibition Act 2015: An Analysis		Perchstone and Graeys Law Firm
			Templars Law Firm

b. Proactively sharing fraud data/information amongst banks and service providers, to enable prompt responses to prevent and/or limit fraud losses and formulating cohesive and effective fraud and risk management strategies, and defining key requirements as relates to e-payment security on behalf of the industry: The Forum has shown clearly its intent in achieving the above through the following actions and regulatory circulars it midwifed;

i. A memorandum of understanding was signed among members which has since facilitated the platform for the industry collaboration that we see today.

ii. The release by the CBN, of three industry defining circulars which include;
   a. Two factor authentication for internal banking processes
   b. Regulation of card present fraud in Non-EMV environment, and;
   c. Creation of fraud desks for effective e-fraud control

iii. The Forum was also able to visit SABRIC (The South African Banking Risk Information Center) and gained useful insight towards setting up a similar protective institution in Nigeria, and also its members attended the World Cyber-Security Summit in Dallas, USA. This Summit no doubt, has deepened the capacity of the Payments Industry to tackle e-fraud, therefore making it poised to respond to the challenges of the times.

1) Delivering on the NeFF mandate – Our Strategies

NeFF has continued on its collaborative efforts aimed at strengthening relationship with law enforcement agencies through a high profile visit led by the Deputy Governor Operations Directorate of CBN, Alhaji Suleiman Barau to the Inspector General of Police, Mr. Solomon Arase. The visit received a huge boost when the Inspector General of Police, ordered the immediate establishment of a Dedicated e-Payment and Card Crime Unit in the Nigeria Police Force at the request of the CBN.

In the same vein, the Chief Justice of Nigeria was visited by the Forum in 2015. This visit also strengthened the Forum's relationship with the Judiciary. At the meeting, the Chief Justice affirmed his commitment to the objectives of NeFF.

The proposed Nigerian Risk Information Centre which aims to reduce bank related fraud through effective public-private partnerships was first mooted at the Nigeria electronic Fraud Forum. The proposal is currently being reviewed by the CBN.

NeFF has been a formidable force for fighting fraud during the year 2015, and a lot of industry initiatives got their genesis from this esteemed Forum. However, as a Forum, we have not stopped strategizing on how to even better this performance.

In October, 2015 the Forum retreated to Uyo in Akwa-Ibom State where a number of strategic plans were conceived and will no doubt turn the tide on fraudsters in 2016.