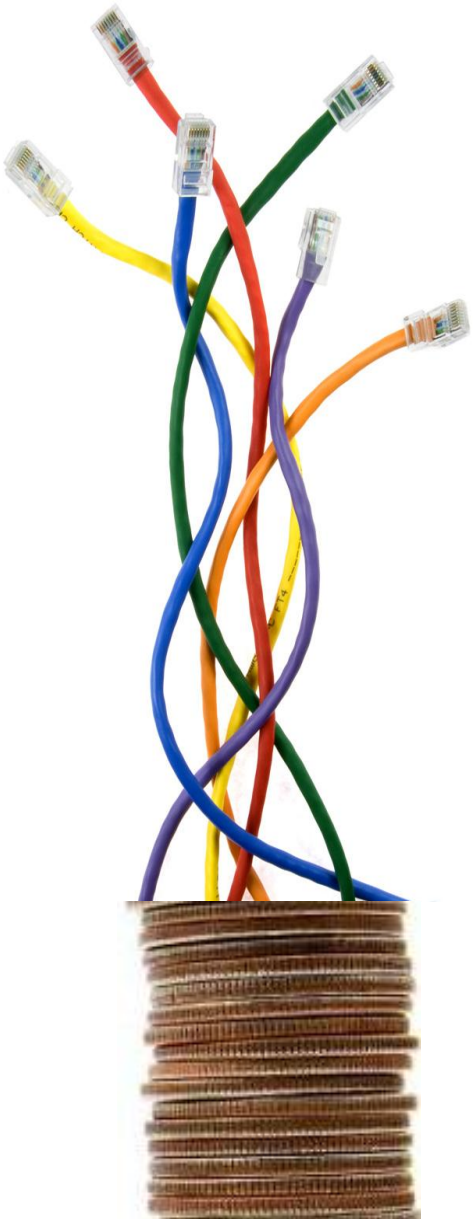
Transferring Risk from Cash to Cashless

Security, Risk Management and Compliance



Presentation at the 2012 Annual Nigeria Computer Society Conference

Tope S. Aladenusi, CISA, CISSP, CRISC, CEH, CIA, ISO27001LA

Head, Information & Technology Risk, Deloitte Nigeria

26 July 2012

Objectives

At the end of this presentation, you will be able to:

- Understand key risks and security concerns associated with the various electronic payment channels of cashless society.
- Understand how we can collectively manage the risks associated with a cashless society.
- Learn from experiences of other countries with more advanced electronic payment channels.

Outline

What-ifs of Cashless Risks

“Everyday in Nigeria, we are building our lives and economy around electronic transactions, the question is, are we ready to work together to ensure the security of our financial information and personal identifiable information, while we manage the risks associated with a cashless society?”

What if …

- … one of our financial institutions was hacked and customer personal identifiable information and financial information were obtained like it was reported in the US on 14 January 2011 that the records (names, addresses, Social Security numbers, account numbers, account registration, transaction details, account balances, and in some cases, dates of birth and email addresses) of about 1,200,000 people were exposed to the web?
  - *Source: Bank Information Security Articles, 2010 Data Breach Timeline, 28 December 2010*

- …our economy faces some negative impact of a 'cashless society' like the cyber experience of the UK? According to a report commissioned by the Cabinet Office into the integrity of computer systems and threats of industrial espionage: Cyber crime costs the UK more than £27bn a year. That's more than Nigeria's 2012 budget!
  - *Source: Guardian Newspaper Article citing* the UK security minister, Baroness Pauline Neville-Jones

- … with the increase in use of POS, we experience a similar thing that happened in the US in December 2011, where Four Romanians were charged for POS Fraud?; the fraudsters remotely hacked point-of-sale and checkout systems at more than 200 merchants to steal card data of about 80,000 Cardholders. The compromised card data is believed to be linked to millions of dollars in unauthorized transactions.
  - *Source:* http://www.bankinfosecurity.com/four-romanians-charged-for-pos-fraud-a-4316

What if …

- … with the introduction of mobile money in Nigeria, we experience a similar event like it was reported in a Ugandan company that lost billions of Ugandan Shillings because fraudsters took advantage of the loopholes in the mobile money system?
  - *Source: MobileMoneyAfrica.com*

- .. with the current increase in the use of the internet for financial transactions, we have a situation similar to this experience in the US?

  "...*Criminals have used the Internet to steal more than $100 million from U.S. banks so far this year and they did it without ever having to draw a gun or pass a note to a teller ...*
  “...I've seen attacks where there's been $10 million lost in one 24-hour period.”

  - Shawn Henry

  FBI Assistant Director, Cyber Division 8 Nov 2010 CBS "60 Minutes"

Is Nigeria in a world of its own?

Certainly not!

If all these data breaches and financial crimes via electronic channels are happening all around the world, do we expect they may not happen in Nigeria with the embrace of a cashless society? What have we done to prevent similar occurrences?

"People who live in glass houses should not throw stones"

We are where the world is …

The Central Bank of Nigeria (CBN) has introduced a ‘cashless’ policy which is to enhance the Nigerian Payment system, reduce the use of cash in payments for goods/services and improve the use of Electronic Payment Systems. The E-payment channels available include:

- Automated Teller Machine (ATM)
- Point of Sale Terminal (POS)
- Electronic Funds Transfer
- Mobile Commerce
- Internet Banking

We are now building a society that is dependent on electronic transactions and now face a plethora of diversified threats and risks like other parts of the world.

From Cash to Cashless – The implications

From Cash to Cashless

Physical crime might decrease with a cashless society, but that doesn't mean crime will decrease. It will just get more sophisticated in nature[1]

Cash

- High Cost of Cash Management
- Insecurity
- Money Laundering
- No Paper Trail
- Transaction Losses due to Fraud
- Counterfeiting among others …

Becomes

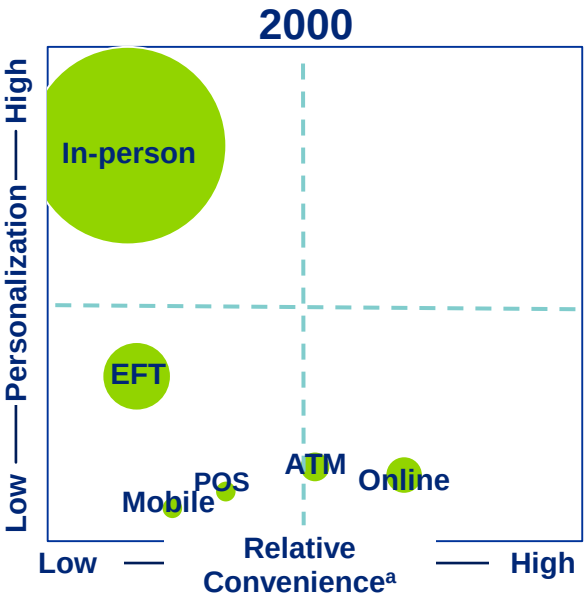
Cashless

- Poor telecommunications infrastructure requiring significant investment
- Lack of User awareness or knowledge gap in operating payment systems
- Interoperability of various platforms
- Diversified security threats from various sources
- Identity theft
- More regulations among others …

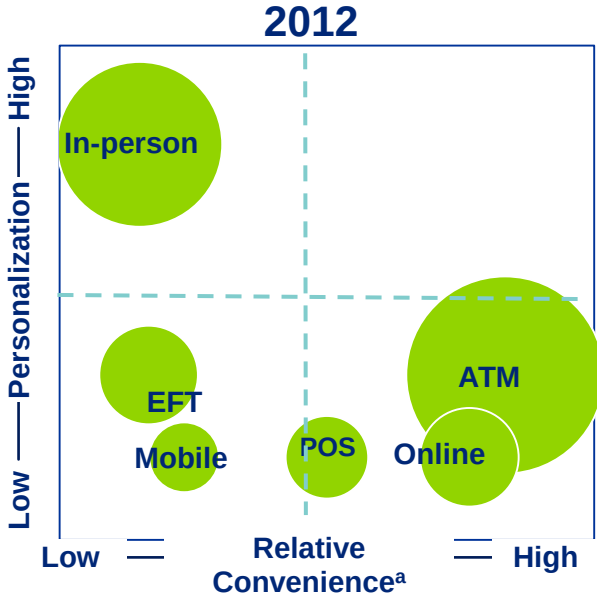
1. Article by Dan Denning - How a Cashless Society Promotes Tyranny, published May 2, 2012 in the Daily Reckoning, Australia

From Cash to Cashless

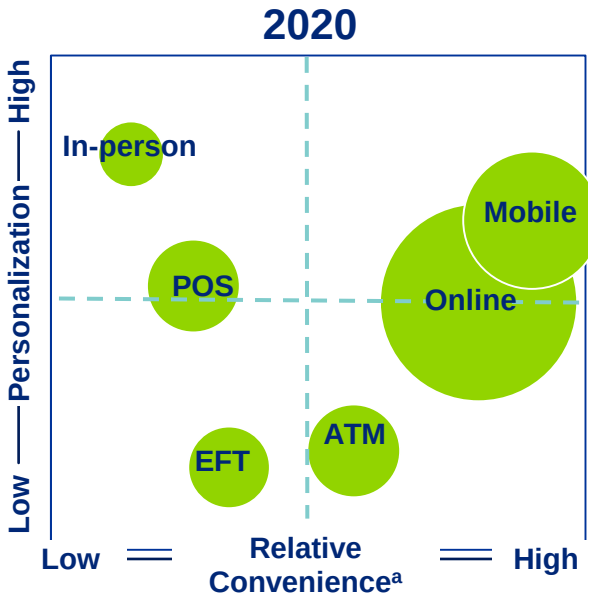
Nigeria Channel Evolution



- Majority of transactions were done in person.



- ATM and transactions through other electronic payment channels are becoming widely accepted.



- Few transactions would be done in-person and most transactions would be through electronic channels.

[a] Convenience is the degree to which a customer can fulfill his banking needs regardless of time and place

Implications

With the embrace of a cashless society, there is a transfer of risk to the various electronic channels, and adequate measures need to be put in place to manage these risks.

References
- Central Bank of Nigeria, Accenture Research
- http://www.cenbank.org/cashless/Cashless%20Lagos%20Presentation_November.pdf
- "Online Banking Report." Financial Insite Inc. Number 162. 22 Jan. 2009

Cashless Risks

Cashless Risks

Payment Channels introduced by the cashless initiative have witnessed increase in systems attacks worldwide and breaches will continue to grow:

– The attacks are becoming more sophisticated

– More breaches are targeted by system components

– Criminals target the easiest opportunities

We would discuss some of the risks associated with the following electronic channels:

- POS
- ATM
- Internet Banking
- Mobile Commerce

POS vulnerabilities

POS devices are usually based on standard PC architecture, therefore they share many of the following vulnerabilities that increases their risk of compromise:

Misconfiguration

- USB and serial administrative ports
- Weak BIOS configuration
- Unnecessary running services
- Missing patches
- Insecure default configurations
- Insufficient audit logging
- Inappropriate file or share permissions
- Inappropriate anti-virus and/or firewall configurations
- Weak password and account policies

By-passing Security

- Availability of protected options that are intended only for maintenance and administrative operations
- Access to “hidden” menu options used for restricted operations on the POS devices
- Some older POS devices even had a backdoor key sequence that was intended only for the vendor to reset or reconfigure the device in the event that a master passcode is lost.

Exploiting Forensic tools

- POS devices store sensitive information in different kind of storage media, including removable media.
- Credit / debit card and transaction data can be extracted from removable media.
- Larger POS terminals in some cases store data on hard drives that may not be securely deleted. Data can be extracted using forensic analysis software tools freely and widely available on the Internet.

ATM Vulnerabilities

Most ATM machines are based on a Windows operating system and have a standard PC architecture which may have vulnerabilities that increases their risk exposure:

Application Vulnerabilities

- Logic errors for “On Us” and/or “Not On Us” transactions
- Inappropriate PIN validation behavior
- Unexpected application response to user error conditions
- Unexpected application response to user cash tampering
- Logging / storage of sensitive customer information or cryptographic material
- Ability of maintenance personnel to bypass application controls

Network Based Vulnerabilities

- Existence of vulnerable and/or unnecessary network services
- Existence of exposed administrative interfaces
- Use of insecure communication protocols
- Existence of permissive firewall rules within the ATM network or VPN terminator

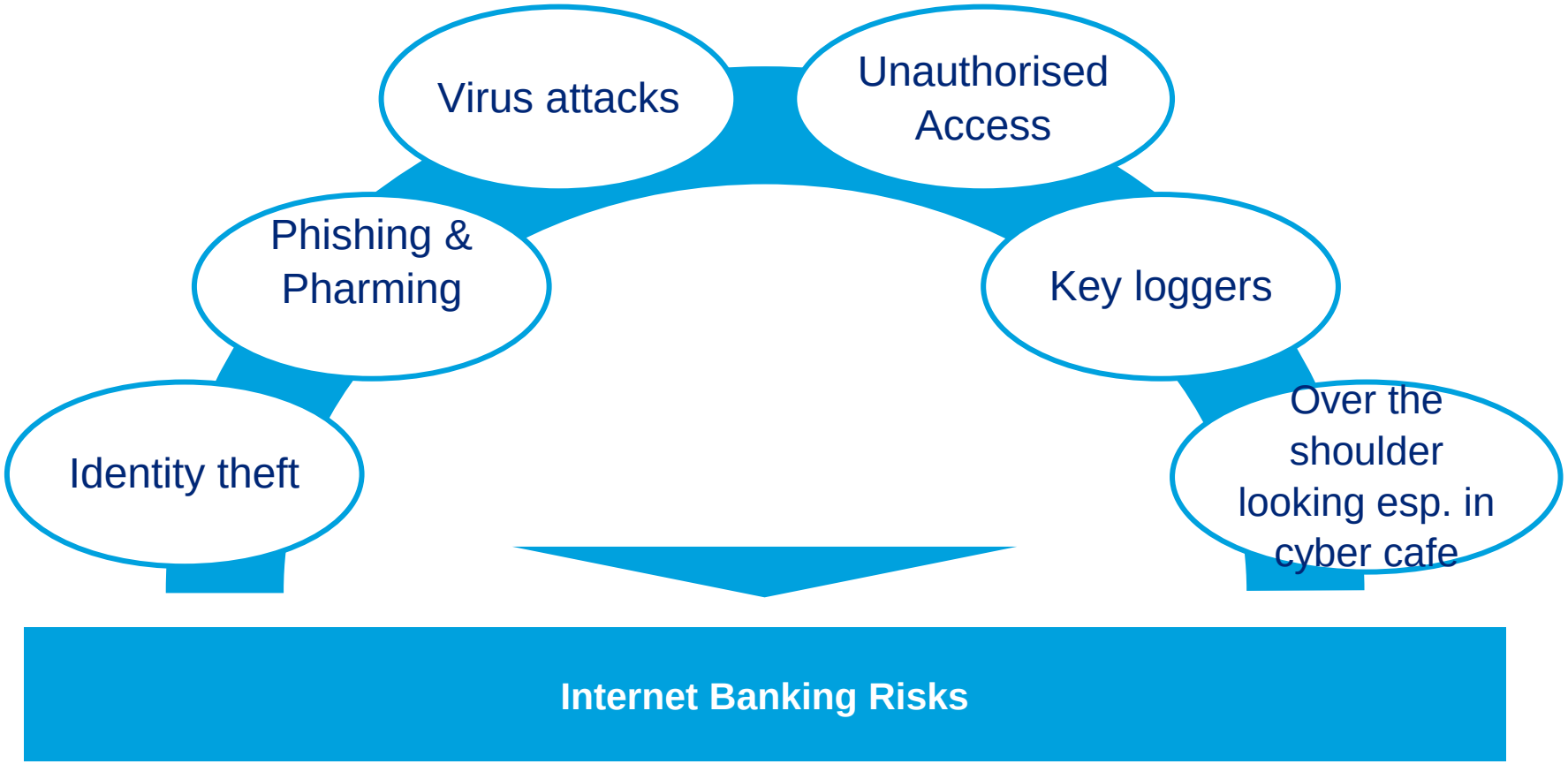
Host Based Vulnerabilities

- Unnecessary running services
- Missing patches
- Insecure default configurations
- Insufficient audit logging
- User account management weaknesses
- Inappropriate anti-virus and/or firewall configurations
- Weak password and account policies
- Weak ATM BIOS configuration

Internet Banking - Risks

Internet Banking also referred to as Electronic Banking (E-banking) is gradually gaining ground, especially by the working class individuals, small and medium enterprises (SME's), because of its convenience, availability (24x7) and typically incurs far less bank fees than going in to a branch to do banking.

However, the risks associated with E-banking are real. They include but not limited to:



Mobile commerce risks

- According to a study by BBC[1], "There are now more than five billion mobile phone connections worldwide."

- With an estimate of over 90 million mobile phone users in Nigeria while only about 25 million Nigerians have bank accounts, experts are optimistic that this will be another revolution in the country's financial landscape.

- But the increasing reliance on smartphones for carrying out financial, business and also personal transactions has made them an attractive target for malware writers.

- At the end of 2010, about 153 families and over 1000 variants of malicious programs targeting mobile devices were revealed[2].

Cyber crooks targeting smartphones: McAfee

- February 2011

19 arrested in $9.5 million Zeus trojan bank scam: Geek.com

– September 2010

Zeus In The Mobile (Zitmo): Online Banking's Two Factor Authentication Defeated: Fortinet

– September 2010

1. Source: http://www.bbc.co.uk/news/10569081
2. Source: Kaspersky Lab (http://www.securelist.com/en/analysis/204792168/Mobile_Malware_Evolution_An_Overview_Part_4)

Mobile Platforms vs. Malware Incidents

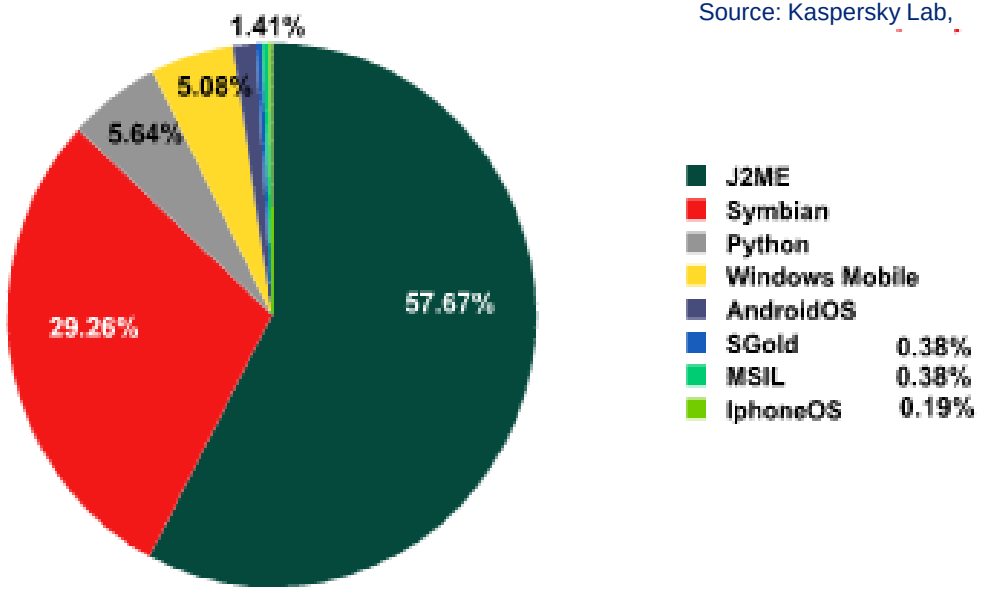
- Just like in PCs, there are a number of vendors in the mobile arena that offer different operating systems. Few of the popular operating systems are listed below:
  - –Symbian
  - –Apple iOS
  - –Android
  - –Windows Phone
  - –Blackberry OS

- Some platforms are currently more attractive targets for malware writers because of the open architecture[1] and the volume of devices in use. However, there are identified malware on other platforms as well.

- Highly standardized, rich, native APIs make malware writing easier and distribution more scalable than on PCs.

- J2ME trojans are the most common among malware writers. Malicious java applications affect not just smartphones but also basic mobile phones[2].

Source: Kaspersky Lab,



The distribution of variants of detected threats, by platform at the end of 2010

1. Source: www.eweek.com/c/a/Security/Android-Malware-Threat-Highlights-Risks-to-All-Smartphones-526196
2. Source: http://www.securelist.com/en/analysis/204792168/Mobile_Malware_Evolution_An_Overview_Part_4

How does it infect my mobile?

Below is non-exhaustive list of vectors that a malware can use to infect mobile devices:

- Bluetooth
- Trojans (concealed within legitimate applications)
- SMS[1]
- OS / App Vulnerabilities
- Removable Storage
- Wifi / Wired Connections
- Device Synchronization
- Email
- Browser
- Over the Air
- GPRS / GSM

1. http://arstechnica.com/apple/news/2009/07/apple-patching-critical-sms-vulnerability-in-iphone-os.ars

Managing the Risks

A collaborative approach is needed

Government

Strong leadership involvement is the foundation for a successfull and effective transition. The Government should:

- Create more awareness.
- Enact adequate regulations. The United States has over 25 Data privacy laws and there are other several privacy laws in different countries[1].
- Monitor compliance with regulations and ensure punishment of voilators. E.g. CBN guideliness for financial institutions to carry out a vulnerability assessment, BCP, PCI DSS compliance, KYC, etc.

IT Practitioners

- Prepare for the worst; Set up adequate incident response team
- Update IT Policy and other relevant policies (e.g. Transaction processing) to reflect the transition to a cashless society.
- Continuous employee awareness.
- Security should be considered at the requirements definition phase and through out the development life cycle of products.
- Ensure technology infrastructures and configurations comply with leading security practices.
- Implement Information Security Strategy and Budget.

1. http://www.informationshield.com/intprivacylaws.html

A collaborative approach is needed

Banks, Merchants & Payment Processors

- Understand that cyber attack is now a matter of inevitability; every bank is likely to be attacked. It's a question of how far it gets.
- Do not view information security as just IT's problem. It is the responsibility of stakeholders from across the business.
- Share intelligence with other financial institutions in a collaborative manner.
- Regular Vulnerability Assessment and Penetration Testing
- Compliance with Leading Standards (ISO, PCI DSS etc). *According to Verisign 2012 Data Breach Report, 96% of victims subject to PCI DSS had not achieved compliance*[1]
- Background check for employees during recruitment.
- Build redundancy into networks & perform real time backups
- Continuous customer enlightment
- Encryption of customer data both at rest and in motion.
- Security should not be an after thought when a product is functional but security should be considered right from the design phase of the product life cycle development.
- Ensure ongoing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) testing program

1.http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

A collaborative approach is needed

Schools

- Information security should be included as a core course in the the curriculum of Information Technology (IT) related courses as some schools offering such courses focus primarily on technology and functionality.
- Secure coding and product development practices should be constantly taught and encouraged.

General Public

Be aware of the challenges and take proactive measures such as:

- Subsribing for sms /email alerts for banking transactions
- Frequently review bank statements for unusual transactions
- Learn to use strong passwords on your email, mobile, iBank, etc.
- Never to disclose PINS, passwords, card numbers or personally identifiable information to people/websites/organisations that one cannot verify as legitimate
- Learn to identify and disregard phishing emails claiming to be from the bank
- Always use up-to-date antivirus and avoid inadvertent installation of “free” programs
- Inform appropriate authorities of suspicious activities.

“A cashless society is indeed very beneficial and appears to be the next best alternative for Nigeria’s payment system. But given that in a cashless society, we trade two major currencies – electronic cash and trust, all hands must be on deck to ensure that we maximize the benefits and minimize the risks.”

Thank You