Economic Cost of Cybercrime in Nigeria

By

'Gbenga Sesan (Paradigm Initiative Nigeria)
Babatope Soremi
Bankole Oluwafemi

This report is part of the output
for the Cyber Stewards Network project
of The Citizen Lab, Munk School of Global Affairs,
University of Toronto, and supported by IDRC.

UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

IDRC CRDI
International Development Research Centre
Centre de recherches pour le développement international

Paradigm Initiative NIGERIA

1 INTRODUCTION

At the turn of the 21st century, Nigerian Internet penetration levels took a running jump. Whereas the number used to be less than 5% in 2002 – 2003, it stood at over 30% by the end of 2012 – and the growth is only poised to accelerate. The advent of mobile telephony on the Nigerian market played a major role and continues to be a key driver of advancements.

The VSAT deployments that were once the only source of dependable internet connectivity have since been rendered quaint and antediluvian, compared to the untapped capacity of the undersea broadband cable that have been brought to the coast of Nigeria since 2009. And as time wears on, competition and market forces continue to act on the industry, constantly nudging quality up and costs down for the average consumer.

However, the rise of the Internet in Nigeria has come with an unintended consequence – global notoriety as a haven of cybercrime. Back in the 90s, fraud in the Nigerian society was popularly called 419 in reference to the penal code that framed the criminal justice system in Nigeria. At the time, persons who were arrested in connection to that law were labeled '419ers'.

Lax criminal law enforcement and a ponderous criminal justice system meant that the rampant practice of 419 was already a constant source of grief. Then along came the Internet, shortly after which a number of tech-savvy cons successfully "exported" the 419 concept. While the popular 419 reference has since been extended to include cyber criminals, in Nigeria the name "Yahoo-Yahoo" is the most familiar informal usage that is employed to speak of people who perpetrate scams online.

2 CYBERCRIME INITIATIVES

Cybercrime is by no means peculiar to Nigeria. It has nonetheless become a persistent source of national chagrin within the comity of nations. Global popular culture continues to associate Nigeria with two things – oil, and princes who promise riches via email. And this notwithstanding, there are those who have, in the country's defence, posited that fraud has no nationality.

Thus, combating the specter of cybercrime and the attendant reputational deficit that it occasions has been high on the national agenda over the past decade. Several initiatives directed at protecting the interests of Nigerians in cyberspace, while laying the requisite groundwork for Information and Communication Technologies (ICTs) that foster development and aid growth in the Nigerian society, have been put forward. Agencies such as the National Information Technology Development Agency (NITDA), Nigerian Communications

Commission (NCC), Economic and Financial Crimes Commission (EFCC) and more, have all worked towards curbing the menace of cybercrime.

A number of Ministries, Departments and Agencies (MDAs) have also been established over the years, to undertake various stratagems towards the end of bringing the problem under control, up to the point where the multiplicity of agencies has led to function and jurisdiction overlaps – and turf wars every now and then.

Some notable cybercrime initiatives include setting up a National Cybercrime Working Group (NCWG) that had stakeholders drawn from the law enforcement agencies, the financial sector and ICT professionals; and a pilot project of a Computer Emergency Response Team (CERT) center by NCWG and NITDA.

3 REGULATORY FRAMEWORK FOR CYBERSPACE

Nigeria's current democracy is fairly nascent. After decades of debilitating military rule, a civilian government was finally re-instated in 1999, marking the beginning of a new chapter in the country's history. With a newly empowered and independent law-making arm, the stage was re-set for many areas of national concern to be given urgent legislative attention.

Since then, cybercrime and cyber security concerns have always had a place on the agenda and have given rise to all kinds of draft legislation on different levels. Some of the draft bills initiated on cybercrime include:

- Computer Security and Critical Infrastructure Bill (2005);
- Electronic Service Provision Bill (2008);
- Interception and Monitoring Bill (2009);
- Cyber Security Bill (2011) – expected to be presented to the National Assembly as an Executive Bill;
- Criminal Code Amendment for Offences Relating to Computer Misuse and Cybercrimes (2011);
- Penal Code (Northern states) Federal Provisions Act, Cap. P3. Laws of the Federation of Nigeria, 2004, to Provide for Offences and Penalties Relating to Computer Misuse and Cybercrimes (2011); and
- Electronic Transfer of Funds Crime Bill (2011).

However, aside from similar purpose and overlapping scopes in many cases, these draft bills all have one thing in common – none of them has made it through to the other side of the elaborate law-making process.

There are various reasons for this. As each legislative session expires every four years, cyber-legislation stakeholders must begin the tedious process all over again – the lobbying, drafting and securing sponsorship of new legislation that will again pass through the Upper (Senate) and Lower (Representatives) houses of the National Assembly.

Another problem is that these efforts are often prosecuted in a haphazard manner, with little or no co-ordination between the upper and lower legislative houses, resulting in all kinds of duplication, and even simultaneous drafts that are at odds.

There are still no clearly defined legislative protocols for protecting Nigerian citizens and assets in cyberspace, as well as securing critical infrastructure without endangering citizen rights or limiting their ability to engage freely online.

4 SCOPE OF RESEARCH

The injury occasioned by Nigeria's cybercrime-induced *reputation deficit* is immense. Many Nigerians are relegated to the status of second-class Internet citizens, denied acceptance and participation in many aspects of the digital economy. Where they are not locked out, they are often made to satisfy unusually onerous conditions that aren't required of non-Nigerians.

Interestingly, as the Internet, mobile technology and electronic transactions are gaining traction locally; ordinary Nigerians who avail themselves of these amenities are also becoming fair game for cybercriminals who are finding it increasingly harder to bilk international targets.

While the effects of cybercrime on the global perception of Nigeria and Nigerians has been explored variously in learned circles, there is little beyond anecdotal evidence on the impact of cybercrime on Nigerian citizens themselves, given the marked uptick in recent incidents of ATM fraud, identity theft, eMail account hijacking, and unsolicited emails promoting financial rewards. The (consumer) economic cost of cybercrime to Nigeria remained unknown until now.

The research scope is focused on gathering data on the economic cost of cybercrime on the Nigerian citizen thus simulating a better grasp of this issue and the need to actively promote proper – firm but fair – legislation.

5 SURVEY METHODOLOGY

The survey was administered both online and offline. Our Offline survey participants were drawn from mainly four locations across the country namely, Abuja (capital city), Abeokuta (South-West Nigeria), Minna (Northern Nigeria) and Uyo (South-East Nigeria). These locations fairly represent the different parts of the country, and relied on the resources of Paradigm Initiative in those locations to get as many responses as possible. The survey was coordinated and administered by selected team leaders, namely **Mayokun Okelola, Unyime-Ben Abasi, Steven Haastrup** and **Titilayo Soremi**.

The survey was administered between February 15 and March 8, 2013, with a total of two thousand nine hundred and eighty (2,980) respondents participating in the survey, online and offline. The exact number of respondents from the specific survey sites is shown in the table below:

Table 1: Number of Respondents per Survey Site

S/No	Survey Site (Region in Nigeria)	No of Respondents
1	Abeokuta (South West)	540
2	Abuja (Capital City)	1,042
3	Minna (North Central)	604
4	Uyo (South East)	610
5	Online/Cyberspace	184
	Total	**2,980**

The survey was designed to be administered in approximately three minutes, with five simple questions to measure respondents' experience with cybercrime incidents, monetary losses, time losses and other losses that might have been occasioned.

6 SURVEY ANALYSIS

6.1 Incidence of Cybercrime

41% of the survey respondents indicated that they had been victims of cybercrime at one time or the other, while 59% indicated that they had yet to fall victim.

Figure 1: Percentage of respondents that have (or have not) been affected by cybercrime

The breakdown of responses by location, shown in Figure 2, indicates higher incidence of cybercrime in the Western and Eastern parts of the country, represented by Abeokuta and Uyo respectively. The northern areas of Abuja and Minna, on the other hand, recorded lower cybercrime occurences.

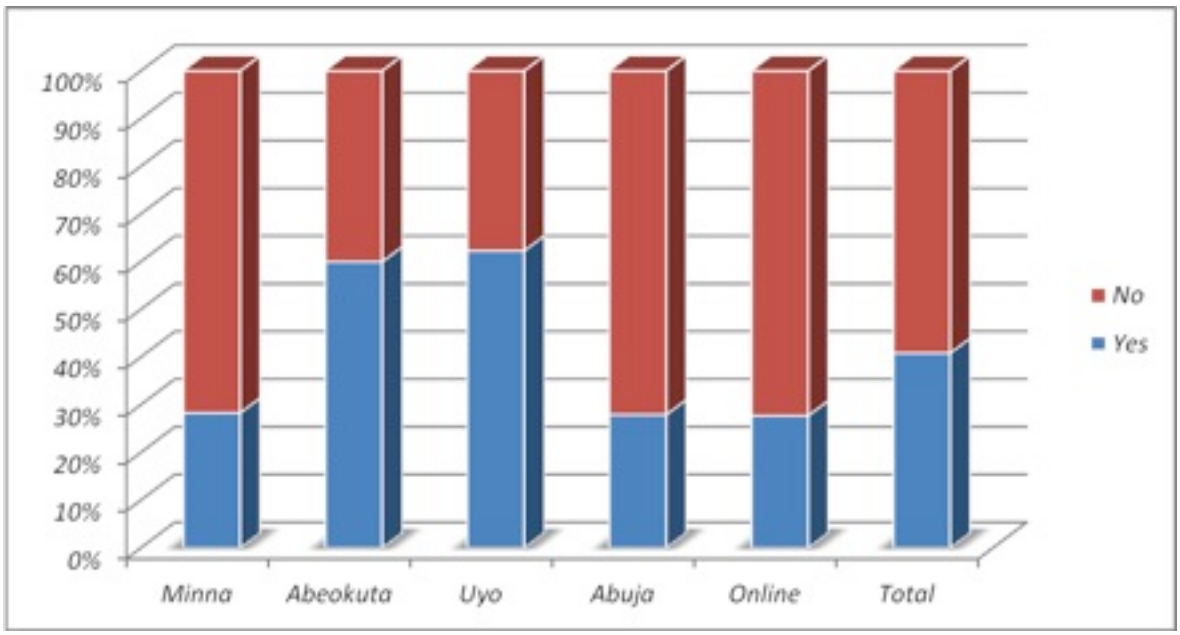

Figure 2: Distribution of cybercrime impact by location

6.2 Incidence of Cybercrime in 2012

70% of respondents affirmed they were not victims of cybercrime in 2012. This is a probable indicator that awareness of cybercrime is increasing, and is causing people to take preventive measures that reduce their vulnerability to attack. The apparent increase in awareness notwithstanding, 30% of respondents fell prey to the vice of cybercrime in 2012.

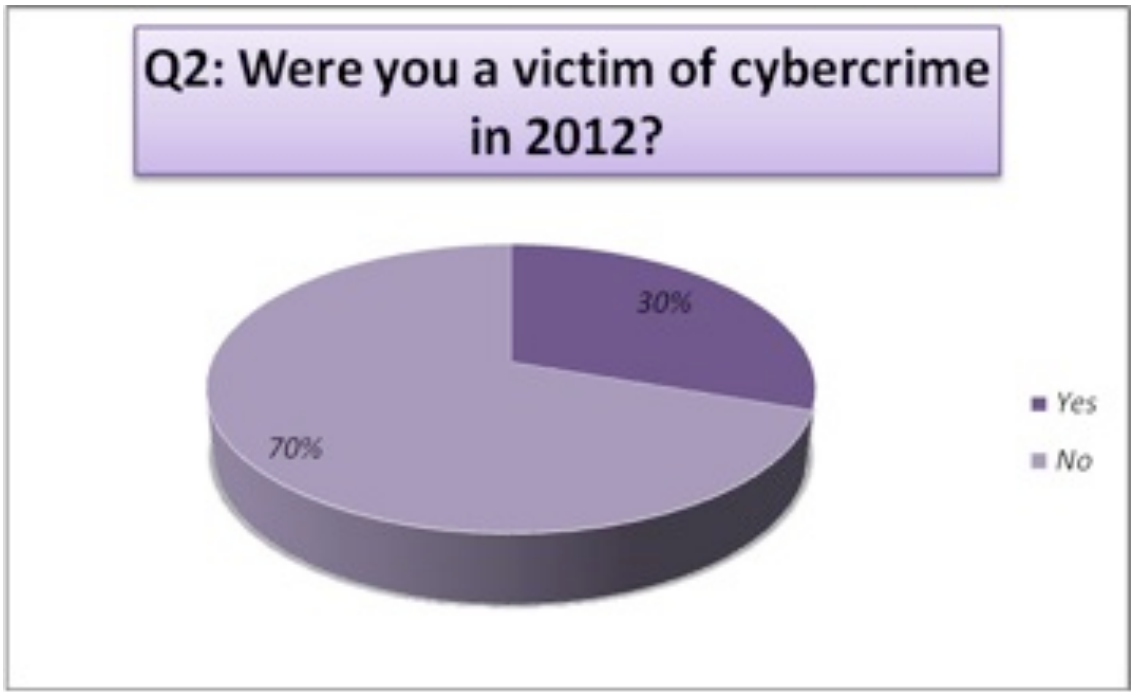

Figure 3: Percentage of respondents that were (or not) affected by cybercrime in 2012

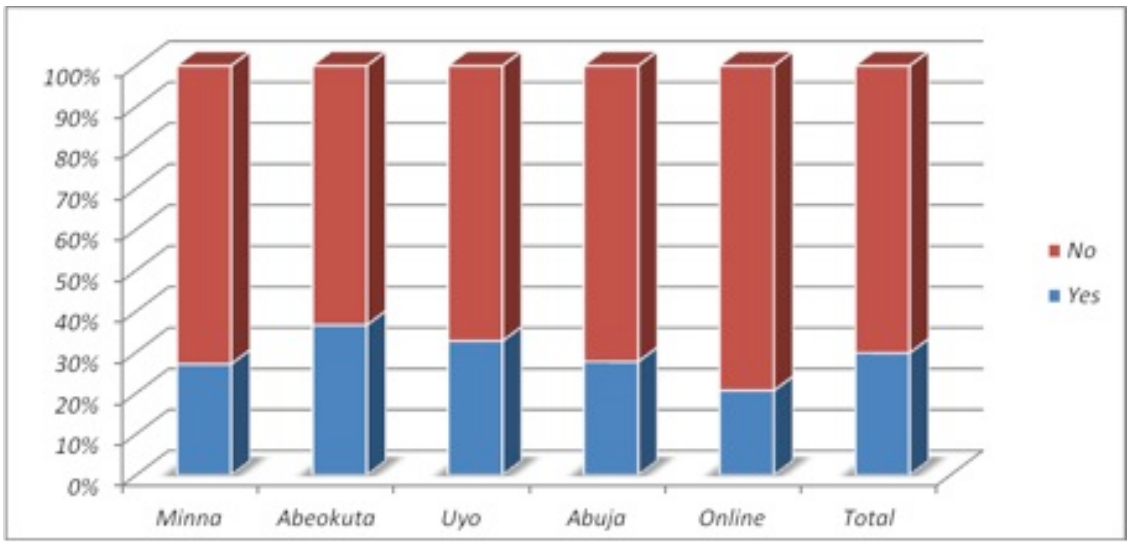

Figure 4: Distribution of cybercrime impact by location, in 2012

Despite a general drop in the event of cybercrime in 2012, Abeokuta and Uyo still recorded higher incidents than other parts of the country. The logical explanation for this would be their relatively higher levels of economic activity compared to the other physical areas surveyed.

6.3 Monetary and Time Losses

The monetary loss sustained by the respondents to cybercrime in 2012 was two hundred and twenty six million, nine hundred and twenty seven thousand, eight hundred and ten naira, and ten kobo (₦226,927,810.10 or $1,432,172.99). 10% of respondents lost more than one million naira (₦1,000,000). 31% of respondents lost between one hundred thousand naira (₦100,000) and nine hundred and ninety-nine thousand naira (₦999,000). 59% of respondents lost less than one hundred thousand naira (₦100,000).

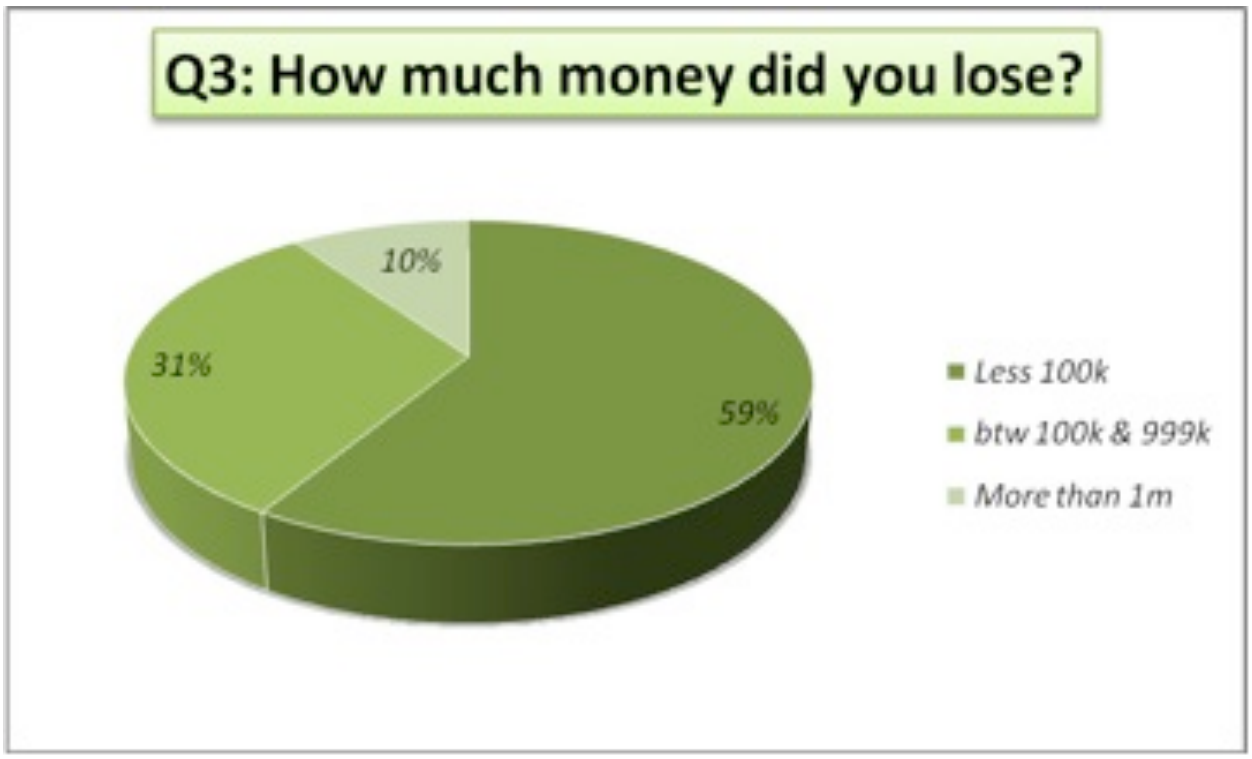

Figure 5: Amount of money lost by respondents to cybercrime, in 2012

6.4 Loss of (Wo)Man-Hours

The loss of (wo)man-hours was another key experience of respondents. 44% of respondents lost over 50 (wo)man-hours. 13% of respondents lost between 11 (wo)man-hours and 50 (wo)man-hours. 43% of respondents lost less than 10 (wo)man-hours. A total of twenty seven

thousand three hundred and seventy one thousand (27,371) (wo)man-hours were lost to cybercrime incidents. This translates to over 3 calendar years.

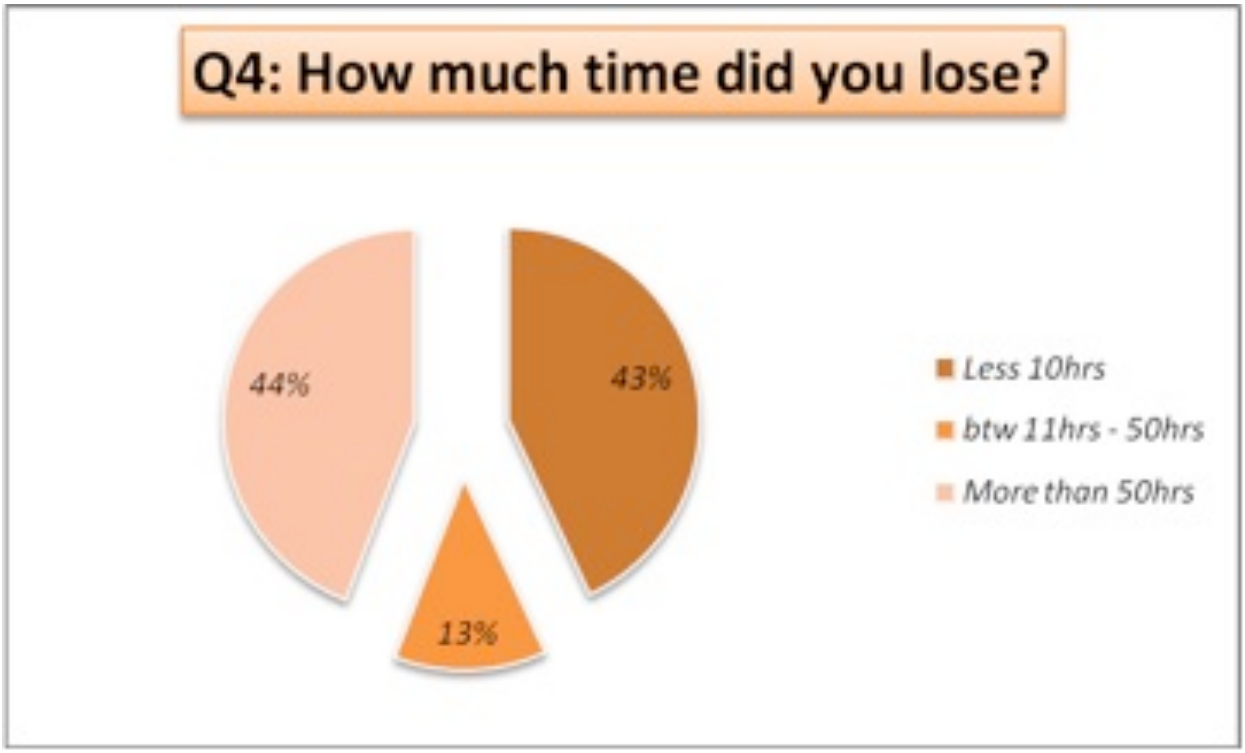

Figure 6: Amount of (wo)man-hours lost to cybercrime incidents in 2012

6.5 Other Losses

Respondents highlighted several other areas of loss they experienced due to cybercrime incidents. The four most common are personal data and effects; phones and airtime recharge cards; goods; and business. For those who lost goods, this included the loss of opportunities to invest, import and/or export their products. Some respondents who had secured visas for sports events and schools also lost the opportunity to complete their trip. The loss of phones by respondents often meant the loss of private information and data that reside on the devices. Loss of personal data was the most common, with banking information ranking highest in this category.

It is also of note that a number of respondents lost property (asset) to cybercriminal activities in 2012. Further details can be seen in Figure 7.

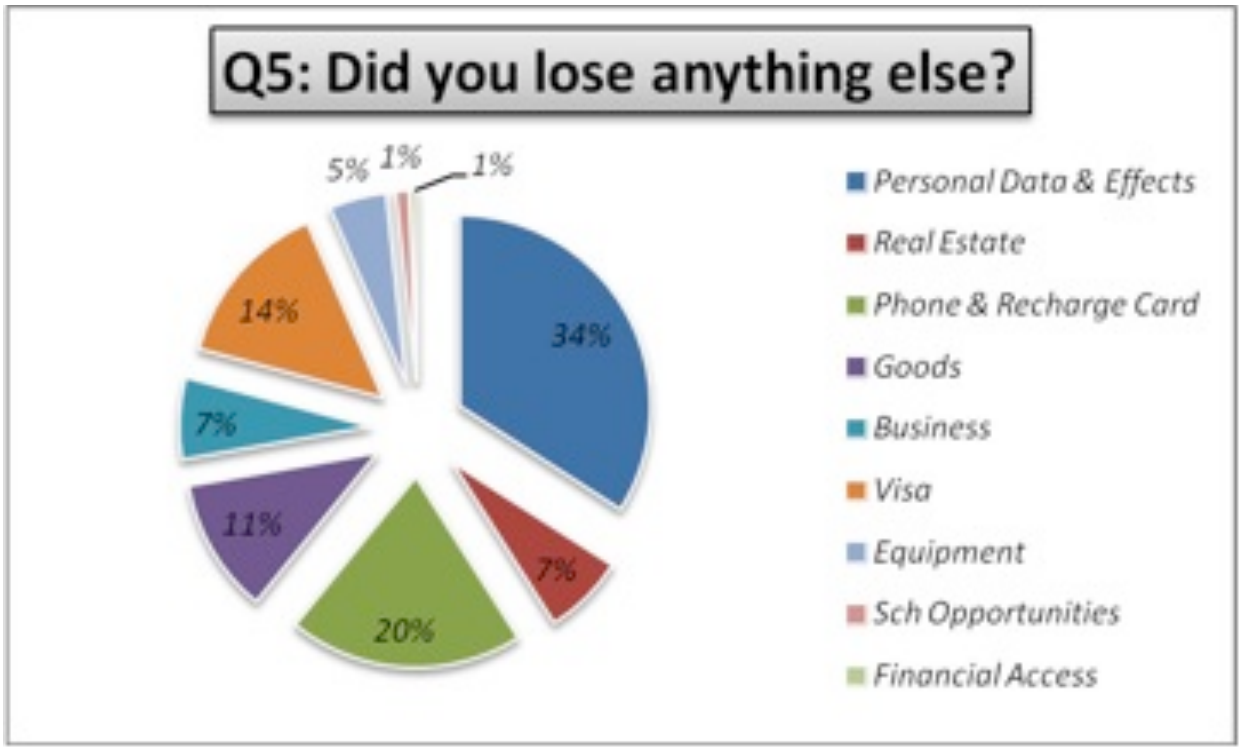

Figure 7: Various non-cash loss reported by survey respondents

7 CALCULATING THE ECONOMIC COST OF CYBERCRIME

To estimate the economic cost of cybercrime in Nigeria, quantitative research was employed in gathering information around losses (money, time and materials) incurred by citizens through cybercrime. Using Nigeria's minimum wage, lost time was computed, and estimates on *Average Revenue Per User* (ARPU) – provided by the telecommunications regulator and others – were used to estimate non-cash, non-time loss. The ratio of Internet users that were affected by cybercrime, calculated from the survey sample size, was then used to estimate the cost for the larger population.

In addition to the monetary losses by respondents, time losses were converted into economic costs using the appropriate fraction of the minimum wage – with each month estimated at 20 working days, and 8 hours per day. The non-cash, non-time loss comprised top-up cards used by victims who called to follow up on their losses, and few cases of reported real estate loss. Based on applicable ARPU in Nigeria, we computed the economic costs of this loss. We used conservative estimates to compute the value of real estate losses.

The cost estimation focused on 2012, so the percentage of respondents that were affected by cybercrime in 2012 was used to estimate how many of Nigeria's 48.3 million Internet users experienced the loss. This was used to compute the estimated loss for Nigeria, noting that

though the sample size for the survey provided 2.36% error margin (and 99% confidence level), only the percentage online are affected directly by cybercrime-related losses. This led to the estimated **Nigerian consumer loss of ₦2,146,666,345,014.75 ($13,547,910,034.80) to cybercrime** in 2012.

8 CONCLUSION

Before now, the economic cost of cybercrime in Nigeria was quantified in intangibles like missed trade opportunities, all as a result of the inherent distrust of Nigerians in foreign countries – and online – occasioned by countless bad experiences. As the foreign targets of cybercrime originating from Nigeria have become considerably less susceptible, it stands to reason that the criminals have begun to look inward to the local population that are relative newcomers to the wonders and vices of cyberspace.

As this report demonstrates, the internal threat is substantial and must be met with concerted deterrent strategy. Else, other new economy initiatives, which are based on electronic interactions – such as mobile money, cashless society, eCommerce, and more – will suffer. Already, the local growth potential of the ICT sector is faced with the growth challenge of a jaded population that has become perennially skeptical of adopting technology in transactional use cases.

In the words of Forbes columnist Peter J. Reilly, "*Nigeria suffers from the fallacy of the undistributed middle, as far as its international reputation for cybercrime goes*". The premise that most online scams in the world emanate from Nigeria is not even close to the truth as it currently stands but no amount of protestations of innocence – or in this case, marginal guilt – can detract from the problem at hand and the responsibility to address it. The problem here is not Nigeria's reputation for cybercrime, but cybercrime in Nigeria – and the attendant economic cost.

Having acknowledged that, it is clear that cybercrime in Nigeria will however continue to remain a problem until legislation that addresses it is passed. Clearly, the current state of cybercrime legislation is not helped by the lack of fervor and conviction that policymakers display when the subject comes up for discussion. It is hoped that the latest set of cybercrime draft bills will not meet the same obscure fate of their predecessors. Considering the huge cost of cybercrime to Nigeria and Nigerians, the need for firm and **fair** cybercrime legislation – that does not hurt Internet freedom – is evident.