Managing Cyber-risk with Regulations

ayo.rotibi@isecureconsulting.co.uk, ayodejirotibi@aol.com

While it is not possible to protect or eliminate the vulnerability of all information and its underlying infrastructure throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks[1].

ABSTRACT

The need for doing business in a more productive way is driving the proliferation of rapidly developing technologies. This development also comes with serious threats which often are ignored or not addressed in the right way or within the required timeframe. Governments and businesses today are facing security threats that would have been un-imaginable only a few years ago. The gap continues to widen between the emerging risks brought out by the rapid development of new technologies and what information security is doing to counter and address these threats. This is even so in an economy as Nigeria where there are little or no national policies, standards, regulations and guidelines for the procurement, deployment and management of cyber-infrastructures

This paper seeks to examine how a regime of regulated cyberspace could serve as a risk management information-centric security models that can support business and strategic goals while protecting sensitive information and lowering costs.

1. INTRODUCTION

The convergence of computers and telecommunication has brought about a new revolution in information technology. Just a few years ago, computers were used to compute, while communication gadget used purely for communication. In the present age, computers communicate and communication gadgets compute. Computers are faster, application software is highly complex and large in size, memory and hard disk size has increased to astonishing levels defying Moore's Law predictions. Computing on the move, Wireless, Blackberry technology, Mobile Phones and powerful laptops are at the forefront of IT technology. Digitalization and globalization have driven the demand for increased flexibility,

[1] HSPD-7 (2003) *Homeland Security Presidential Directive / HSPD-7* http://www.fas.org/irp/offdocs/nspd/hspd-7.html

scalability, and availability of information, which is changing the way organizations are viewing information security. This revolution enhances operational functionality, improves data availability, and optimizes business performance and changed the way governments and businesses operate, with most national economies and security becoming fully dependent upon information technology and its underlying information infrastructure.

The increasing reliance upon the convergent technology and network infrastructure has introduced new variants of risks to national security, governance and business processes. Information and its underlying infrastructure have come under persistent threat of attacks and sophisticated information warfare. Information Security therefore exists to manage this risk.

Given the economic risks associated with a concerted cyber-attack on a nation, governments the world over introduced Risk Management Framework in the form of regulations that seek to protect and defend information of national importance. Cybersecurity is therefore a shared responsibility of government, business, other organizations, and individual users who develop, own, provide, manage, service and use these information systems and networks. Managing the inherent risks requires that the participants act cooperatively and in coordination with one other, and that each participant take action to address security appropriate to its role. The collective goal of participants is to prevent, prepare for, respond to, and recover from incidents. In this interconnected system, the roles and responsibilities of participants for Cybersecurity are shared and often overlap. Only when all participants share a common vision and understanding of the security objectives and how to achieve them, as well as their individual roles in the effort, can the collective goal be achieved.

2. CYBERSECURITY

Cybersecurity and information security are synonymous, especially in national government circles. The entire Cybersecurity industry is an accident: an artefact of how the computer industry developed[2]. Traditionally, computers are hard to use; you need an IT department

[2] Bruce Schneier: *The Death of the Security Industry* (2007)

staffed with experts just to make everything work. Contrast this with other mature high-tech products such as those for power and lighting, heating and air conditioning, automobiles and airplanes. No company has an automotive-technology department, staffed with engineers needed to install the latest engine upgrades and help users recover from the inevitable crashes.

Due to reliance on energy and telecommunications in today's interconnectedness of global economies, the nature of risks and vulnerabilities is becoming increasingly trans-national, defying functional or geographical boundaries. Trainor[3] reported how the 1998 failure of Galaxy IV Satellite affected over 45 million (pager, radio and television) customers in the United States, and the Chinese Television Network in far away Hong Kong. Barely eight months earlier, the President's Commission on Critical Infrastructure Protection in the USA found reasons to step up Cybersecurity[4] . However, the watershed of Cybersecurity in the USA (and many other IT-dependent nations) was the Executive Order 13231[5]; an aftermath of the attack and destruction of the World Trade Centre in September 2001.

Homeland Security Act defines the term `*Cybersecurity*' as the prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation[6]. This information must not be disclosed to anyone who is not authorized to access it and the system must not corrupt the information or allow any unauthorized malicious or accidental changes to it. There are three aspects to integrity: authorized actions, separation and protection of resources, and error detection and correction. In order for the system to be usable, the services provided by it must be present in an obtainable form. Aspects of availability include: presence of object or service in a usable form, capacity to meet service needs, and adequate time/timeliness of service.

[3] Trainor, J. *May 1998 Satellite Failure* [online] Available from: http://www.zetatalk.com/theword/tworx516.htm
[4] PCCIP (1997) *Critical Foundations: Protecting America's Infrastructures* http://www.fas.org/sgp/library/pccip.pdf
[5] EO-13231 (2002) *Critical Infrastructure Protection in the Information Age* http://www.ncs.gov/library/policy_docs/eo_13231.pdf
[6] Homeland Security Act, (2004)

2.1 CYBER ASSET

Information has been defined as data with *meaning, relevance and purpose*[7]. Without these attributes, expending resources to protect it is of little justification. In other word, the value of the information asset determines the level and cost of protection. Knowledge is created from information and it is, in turn, captured, transported and stored as organised information asset. Various parties persistently contend for this asset: The owners *value* it and therefore wish to *minimise* the *risk* of exposure by imposing *countermeasure* in the form of self-imposed or regulator-imposed controls; the countermeasures may bring about some other known or unknown vulnerabilities that may be reduced or treated by some other controls. At the same time, the threat agents wish to compromise and abuse the asset by launching cyber-warfare which gives rise to threats to the asset. Figure 1 below depicts these cyber-activities.

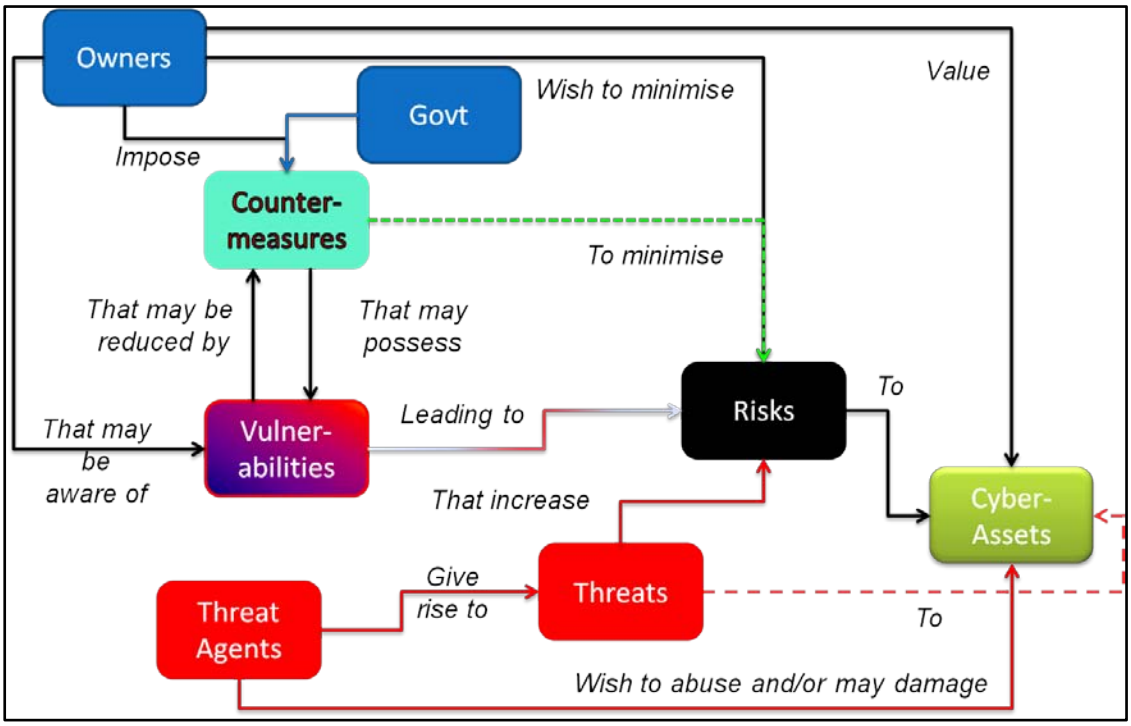

Figure 1: Cyber-activity to Cyber-assets

[7] ISACA *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition,* (2006)

3. RISK MANAGEMENT

Business rewards comes from taking risks; managed, controlled risk taking, but risk taking nonetheless. The business environment has always been full of threats, from employees, competitors and external environment. Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence, a function of the likelihood of a threat agent exploiting a particular potential vulnerability. Risk Management is a C-level issue that continuously identifies and assesses risk, and applies controls to reduce risk to an acceptable level, and maintaining that level of risk. Commentators and policy-makers debate whether risk controls should be 'rational' or 'social' – where the former approaches tend towards Cost-Benefit analysis and the latter emphasise participation and negotiation between lay persons and experts. It is accepted in many circles that risk controls cannot be designed on a purely rational basis. Risks can be controlled within organisations through techniques of management or they can be regulated by the imposition of constraints from outside the institution performing the primary function. In the UK, the Cabinet Office insists that all regulatory proposals put forward by government officials be supported by a Compliance Cost Assessment (CCA) accompanied by a risk assessment. The risk assessments seek to: identify the problem and the harm involved; estimate the risk associated with the harm (this involves assessing the probability or frequency of the harm arising as well as its likely magnitude); identify regulatory options; estimate the impact of the options on the risk; place a monetary value on the expected benefits of each option; compare the costs with the benefits; and identify any important issues of equity or other political considerations. This effort guarantees that the proposed control benefits the business.

Essential to Risk Management strategy are the following:

a. Organization seeks to clearly understand the amount of risk it is willing to take in order to meet its business objectives. The ultimate purpose is consistent interpretation of risks across the organization to formulate a reliable decision-making process. While determining its risk appetite, an organization must decide on regulatory compliance and standards, assess current risk status and vulnerabilities and prioritize risks based on impact.

b. Organization seeks to remain in business even when under attack, and to recover after an attack. Security breaches, unintentional loss of IT assets, accidental deletion of critical data, or power outage in a data centre are examples of incidents that require comprehensive incident management and disaster recovery planning. Business continuity and disaster recovery planning allows organizations to respond swiftly in crisis situations and protect ongoing operations. To ensure this resilience in case of incidents, organizations must periodically perform business impact and environmental risk analysis and test the recovery plan.
c. Organisation wishes to convert risk assessment into data to drive decision-making using a risk database.

These points are of great relevance when considering a regulatory regime.

4. CYBER REGULATION: APPROACHES

Cybersecurity regulations are interventions that acknowledge the possibility of an attack; and therefore provides for the integration of detection and recovery processes into protection process of the traditional information security. Objectives of such intervention include: to minimise the probability of vulnerability; to minimise the damage due to vulnerability exploit; and provide efficient recovery methods from damage. For the realisation of these objectives, three basic concepts are identified namely: Access control, Individual accountability, and Audit trails. Built upon these concepts are four models namely: the Information Value (IV) model, The Need-To-Know (NTK) model, the Confidentiality-Integrity-Availability (CIA) model, and the Protect-Detect-React-Deter (PDRD) model[8]. In the real world of cyber operation, a combination of these models is employed. In its effort to develop a policy roadmap for Information protection in Europe, The Dependability Development Support Initiative (DDSI), an EU-supported Information Society Technologies project, argued that *dependability* (which includes such attributes as Availability, Reliability, Safety, Confidentiality, Integrity, and Maintainability) is a valuable concept in dealing with risk to information infrastructure, and that information risk management underpins Information Assurance[9].

[8] Blyth, A. and Kovacich, G., (2006) *Information Assurance: Surviving in the Information Environment*, London: Springer
[9] DDSI, (2002) *DDSI-IST-2000-29202* http://www.ddsi.org/Documents/final%20docs/DDSI_D1_concept_paper_f.pdf

Below are a few of the approaches taken by countries to address Cybersecurity:

(i) a legislative approach;

(ii) a regulatory approach;

(iii) a self-regulated approach;

(iv) an incentive approach;

(v) a disclosure approach; and

(vi) Insurance mechanism.

For the purpose of this paper, I will dwell a bit more on some of these approaches.

4.1 Legislative Approach

The legislative approach regulation is characterised by the use of rules reinforced by legal sanctions. Required behaviour is stipulated, standards are fixed, unacceptable actions are defined and outlawed and penalties for noncompliance are set out. Legislative approach derives strength from the use of law to designate what is acceptable. Its alleged weaknesses are that it involves high levels of intervention in management; it is marked by complex rules and "red tape"; and it only demands compliance with a stipulated standard rather than the best level of risk avoidance that is reasonable in a particular context.

4.2 Regulatory Approach

Under the regulatory approach, countries do not develop new legislation to address Cybersecurity. Instead, they modify existing regulations or institute new regulations to address new technologies. This approach can be a practical way of addressing Cybersecurity provided that existing regulations can be modified or new ones introduced relatively quickly. However, the regulatory approach must be carefully managed to minimize inconsistencies between new and existing rules. Given the rather slow pace of work on the various Cybersecurity initiatives with the Nigerian National Assembly, one would imagine that the regulatory approach will be used by the NCC in conjunction with the legislative approach because the complementary mix allows governments to establish new legal frameworks to address convergence while dealing with its specific effects through regulation.

4.3 Incentives Approach

Governments may control risks by adjusting economic incentives. Such regimes are welcomed as involving low interference with managerial freedoms, as involving incentives to reduce risks to zero (not to a given standard only) and as requiring low cost enforcement. They are criticised on the grounds that they assume a high degree of rationality from the regulated (whereas many risks flow from irrational, ill-informed actions.)

4.4 Disclosure Approach

Risk controls can be imposed by requirements that operators or service providers, supply information to the public concerning their products and businesses. Consumers or state institutions may then decide whether to purchase high risk/low cost or low risk/high cost products. Such controls involve low levels of intervention, can be said to be highly democratic and may be useful where risks are low and more strongly preventative measures are not called for.

Each of the approaches presents advantages and disadvantages, but no one approach results in an optimal solution (ITU, 2012). In general, countries see more effective results when several approaches, especially the legislative and the regulatory ones, are used together. Moreover, the first two approaches are generally more effective when they also incorporate a consultative process, such as the various public hearings organised by the NCC in the past.

Regardless of which approach, questions remain: is regulation good for information security? Good for Nigeria? Can we do it in a way that will have an actual impact on security and the bottom-line of every enterprise? Security experts have mixed opinions about whether regulation has a positive impact on the sector and on business. To answer these questions, we will consider the advantages and disadvantages of cyber-regulations and a case study.

5. CYBER REGULATION: ADVANTAGES AND DISADVANTAGES

From the perspective of business alignment and bottom-line, regulation has advantages and disadvantages.

5.1 Advantages

Below are a few reasons in favour of regulation:

5.11 Improved Security

We can debate how much improvement regulation actually can provide and the extent to which improvement will unfold over time. However, it is common knowledge that regulation improves quality and security because it *forces* those who don't do anything to at least do something. The question is how much? The reason is simple— many companies have little information security protection beyond a firewall and antivirus software. There is so much room for improvement that we're likely to achieve even if we do a bare minimum as stipulated by the regulation. Remember the due-diligence we mentioned above about the UK Cabinet office insisting that all regulatory proposals put forward by government officials be supported by a Compliance Cost Assessment (CCA) accompanied by a risk assessment showing the benefits including Return-On-Security Investment (ROSI).

5.12 Positive Economic Impact

If it can be demonstrated that security regulation adequately addresses security concerns, publicly disclosing this information would provide comfort and confidence to consumers, corporate investors, and the government.

5.13 More Sophisticated Security Awareness

Regulation makes any topic a Board and Executive management-level issue. There is little question that getting corporate management and boards of directors to understand information security's risks and rewards will elevate Cybersecurity from operational and technical to more strategic and C-level issue.

5.2 Disadvantages

On the other side, there are minuses to consider.

5.21 Cost

Regulation costs money: money to comply, audit and regulate the compliance. Such expenditures affect ROSI and other bottom-line results. In a 2009 survey by Ponemon Institute LLC on PCI-DSS Compliance, on average, companies spent about a third of their budget on PCI-DSS. The average IT security budget was approximately $15 million, meaning most companies spend about $5 million on PCI-DSS compliance only[10].

5.22 Disagreements about metrics

Security experts disagree over security metrics. Simply put, we don't know what to measure and how much of whatever we need to measure is sufficient to call a system secure. Security is a process, not a product, and there are always things that we can improve. How do we set the passing-grade bar high enough to produce reasonable confidence but low enough to be affordable? How do we calculate ROSI?

5.23 The lack of definable boundaries

Cybersecurity is an international issue. Today's networks do not have physical boundaries. In fact, the Internet is available in countries even while they are at war. All of this makes implementing regulations to protect our country a difficult proposition.

5.24 Introduction of new risk

New laws and regulation may introduce new risk to the system. Legal penalties associated with non-compliance with relevant legislation can create additional risks that are attributable solely to that legislation. Risks can relate to fines for non-compliance with legislation; imprisonment for senior executives; and brand damage associated with bad publicity.

5.25 Inconsistent asset value

Legislation can give information asset a value that may be different from that identified by a risk assessment. For example, the EU privacy laws require personally

[10] Ponemon (2009) *PCI-DSS Compliance* http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/IBM%20Business%20Case%20for%20Data%20Protection%20UK%20White%20Paper%20FINAL6%20doc.pdf

identifiable information to be treated as having a high value and degree of protection, regardless of how valuable it is to the organisation.

5.3 Case Study

These advantages and disadvantages raise some seriously thorny issues. The strong points on both sides of the issue exacerbate the problem of arriving at an informed opinion. So, what is a security person to do? One worthwhile exercise involves comparing how the Year 2000 Problem was managed from a regulatory perspective with the consequences of non compliance to a security standard.

Until the US' Security Exchange Commission (SEC) adopted a new temporary rule requiring companies to file specific reports on their Y2K readiness and established a schedule of fines for non-compliance, only a few corporations were working actively on it. An estimated US$100B was spent on Y2K in the US[11]. At the turn of the millennium, nothing happened; the heaven did not fall and the SCADA systems did not fail. Some critics called into question how technologist could be so wound up spending over $5 trillion worldwide on a problem that seemingly fizzled out. The irony is that it was the regulations and mitigation exercise that made sure that nothing happened.

On the other hand, when in January 2007 TJ Maxx announced that 45 millions of customers' credit and debit cards might have been affected by a data security breach that was undiscovered for two years, it was the biggest data breach ever. To make matters worse, *Wall Street Journal* reported that the $17.4-billion retailer's wireless network had less security than many people have on their home networks, and for 18 months the company had no idea what was going on as it failed to secure a wireless network at a discount store. It was suggested that TJX might have been ignoring even basic security rules for years, and even ignored the PCI-DSS security standards introduced by the credit card industry to avoid such breaches. While most organization that take credit cards use some form of encryption to protect data during and after the transaction, it appears that not only were the TJX thieves able to intercept customer credit card data before it was even encrypted, the bad guys already had a copy of the encryption key anyway. According to one security analyst "it's like locking the door and leaving the key under the mat." In other words, TJX did not in

[11] Y2K Spending: http://en.wikipedia.org/wiki/Year_2000_problem

actual fact *own* the data in its custody. It was estimated that the security breach cost TJX over $8.6B in fines, compensation and legal charges[12] – so much to pay for ignoring a security regulation standard that was developed to prevent such incident.

In both cases, there were regulations to guide on how to avoid losses, secure businesses and guarantee continuity. The first case cost so much but no major incident was recorded, the second case resulted in a major incident, although TJX never made public how much it spent on security prior to the incident, one can only draw conclusion on the available information: that TJX did not follow due-diligence in its security operations.

6. CYBER-RISK AND CYBER-REGULATION IN CONTEXT

Every business, regardless of maturity or industry, faces a wide variety of risks. These risks come in many forms, including market risks, financial risks, legal risks, and more. One of the most challenging areas is the risk associated with information and information systems – cyber risk. Virtually every business today is facing cyber risks, ranging from the loss of information on a single laptop to disruption of its entire business due to a data centre outage, and the cyber risks that a business encounters are constantly changing. Today, protecting the security of corporate information and computer systems is no longer a technical issue to be addressed by the IT department, but a legal obligation directly on the shoulders of senior management, and in many cases the board of directors. It is, in many respects, a corporate governance issue. Under the Sarbanes-Oxley Act[13], for example, responsibility lies with the CEO and the CFO. In the financial industry, the Gramm-Leach-Bliley (GLBA) security regulations place responsibility for security directly with the Board of Directors[14]. In the healthcare industry, the HIPAA[15] security regulations require an identified security official to be responsibility for compliance. The scope of that responsibility can also be significant. The GLB security regulations, for example, require the Board of Directors to approve the written security program, to oversee the development, implementation, and maintenance of the program, and to require regular reports (at least annually) regarding the

[12] http://www.v3.co.uk/v3-uk/news/1952558/tjx-counts-continued-cost-breach
[13] Sarbanes-Oxley Act, Section 302
[14] GLB Security Regulations (Federal Reserve) 12 C.F.R. 208, Appendix D-2.III(A)
[15] HIPAA Security Regulations, 45 C.F.R. Section 164.308(a)(2)

overall status of the security program, the company's compliance with regulations, and material matters relating to the security program[16].

Most of the security laws and regulations recognise the relativity of security. They contain such clauses as "reasonable" and "appropriate". Both the ISO/IEC 27001[17] and the UN Convention on the Use of Electronic Communications in International Contracts[18] expressly adopts the view that security is a relative concept. This concept therefore allows for the adoption and implementation of the security law based on the value attached to the asset.

In a 2005 survey by Information Security Ltd, the most common drivers for organisations that have historically, been successful in achieving BS 7799 (ISO 27001) in the UK, "were commercial: to increase the confidence of customers, or possibly to encourage suppliers, when dealing with the organisation" For others, an information security standard is "becoming and increasing requirement in tender documents, as well as contracts.[19]" Similarly, In a 2010 survey by Ponemon Institute LLC on 115 UK-based C-level executives, 51% believe data protection programs increase or maintain their marketplace reputation and brand and another 40% believe the program increase customer trust and loyalty. When asked what are the most important activities for a data protection program, 76% believe it is reducing potential security flaws within business-critical applications, 71 percent say training of employees, temporary employees and contractors and 67 percent of respondents believe it is a data protection strategy[20]. To another survey question, C-level executives believe data protection programs yield an excellent ROI; they unanimously agreed that the cost savings from investing in a data protection program of £11 million is substantially higher than the extrapolated value of data protection spending of £1.9 million; suggesting a very healthy ROI for data protection programs.

6.1 Nigeria: Cash-less Policy and ATM Cards

Finally, the use of cards for transactions arrived Nigeria. Reading the Cash-less Policy, one noticed the good intention of the Central Bank of Nigeria (CBN); "*to drive development and*

[16] GLB Security Regulations (OCC), 12 C.F.R. Part 30, Appendix B, Part III.A and Part III.F.
[17] http://www.iso.org/iso/iso_catalogue.htm
[18] http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2005Convention.html
[19] Information Security BS7799 Survey 2005 – Information Security Ltd
[20] http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/IBM%20Business%20Case%20for%20Data%20Protection%20UK%20White%20Paper%20FINAL6%20doc.pdf

modernization of our payment system in line with Nigeria's vision 2020 goal of being amongst the top 20 economies by the year 2020[21]" This will introduce POS too. However, there is no public information on the guidelines to secure the online transactions. In a survey conducted by *BusinessDay Newspaper* on 350 respondents classified into Top/Middle and Lower segments, 57% of Top/Middle respondent believed the policy will enhance business. In contrast, 50% of Lower segment respondents responded to the negative[22]. Respondents were also asked if they have ATM cards and use them. An average of 73% of the respondents said they do. As good as this acceptance looks, one wonders if any of the banks and issuing houses is subjected to the PCI DSS standard or regulated by any Cybersecurity policy for that matter. Same goes for the Mobile Money initiatives. All of these initiatives are increasingly dependent on ICT. Such is a challenge that NCC and other relevant agencies would need to regulate urgently. "If it is not written down, it did not happen" so goes the popular saying. Although there are standards for compliances in some sectors, the present business settings and patronage in Nigeria do not make provision for compliance to international standards of information security. Particularly, ISO/IEC 27001 outlines the code of practice for information security management (security techniques), which most businesses are requested to comply with. While the relevant legislations for such compliance are being promulgated, major players in the Cash-less initiatives, ATM card issuing houses and Mobile Money operators could be requested to have organisational commitment statement, signed by the CEO or Board Chairman, outlining their commitments to a Cybersecurity regime and verifying their responsibility for sustaining security measures on their individual network.

6.2 Common areas of the law relevant to information security

When asked to scale the relevance of the various regulations to information security, Members of the Information Security Forum (ISF) identified data privacy and financial regulation as being particularly relevant to information security. The percentage of

---

21 http://www.cbn.gov.ng/out/2011/pressrelease/gvd/CASHLESS%20LAGOS%20BRIEF%20FOR%20WEBSITE%20revised2.pdf

22 http://www.businessdayonline.com/NG/index.php/analysis/features/33680-what-nigerians-think-of-the-cash-less-economy-policy-

Members identifying these common areas is shown below[23]. Topics are grouped as information security-specific legislation (shown in red); general legislation with security implications (shown as orange) and regulatory legislation (shown as green).

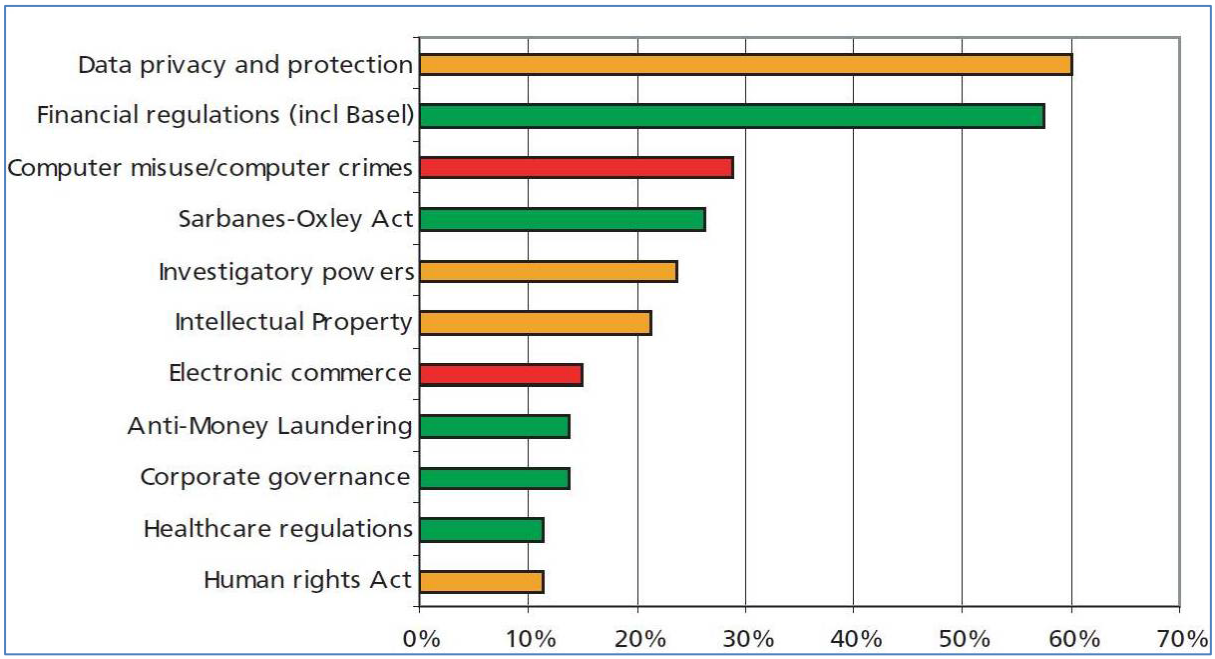

Figure 2: Laws/Regulations relevant to information security

6.3 Case Study: PCI DSS

Credit card brands are aware of the fact that compromised data can cost a lot of money. They are also conscious that data breaches can turn into identity theft cases affecting the reputation of their industry. This is especially harmful since the industry could lose plenty of its gains if people start thinking that credit cards are not a safe way to handle their finances. In order to minimize the risk of having card/cardholder data compromised, the Card industry introduced PCI DSS; a Security Standard with the sole objective to protect cardholder data. Its *requirements* should be applied on any system, server and/or network containing cardholder data such as Principal Account Number (PAN) or Card Number, Cardholder Name, Card Expiration Date, Service Code, Full magnetic stripe data (CAV2/CVC2/CVV2/CID1) and PINs/PIN blocks. Hence, for any organization that transmits, processes and stores payment card information, protection of that information is no longer

[23] Information Security Forum: *Security and Legislation Overview* (2005)

a second thought, but a top priority. The non-compliance to this regulation can result in costly penalties. Of the 12 *requirements*[24] included in the standard, at least six falls under business as usual (BIU) for the Network Administrator; they are simply due diligence process that many of us engage even for our individual devices and home network. The cost of compliance to this standard varies widely between $80,000 for a Level 4 merchant and over $2 Million for a Level 1 merchant. This does not include yearly audit or IP scan cost. This cost significantly affects the bottom-line. However, for a cumulative number, Gartner estimates that the cost of a data security breach can range from $90 to $305 per customer record[25]. Security incident where 100,000 records are compromised can cost a company a minimum of $90 Million (not including fines and legal cost). Basic computation reveals that the cost of compliance is far less that the cost of a security breach.

6.4 Case Study: Aftermath of 9/11

Before September 11, anyone who had ever tried to persuade an organization to part with money to fund disaster recovery and/or business continuity requirements was quickly met with resistance. Some of the organizations affected by the 9/11 disaster have, to varying degrees, invoked disaster recovery plans, other did not have any such plan. In effect, many companies; especially financial institution struggled to cope in the days immediately following the bombing, and some are yet to recover till this very date. However, some were back in business and restored online activities within days after they invoked there recovery plan – one of the Controls included in ISO/IEC 27001.

7. SUGGESTIONS

In Nigeria, it is difficult to give any reliable answer to the question of how much cybercrime there is on the Internet as there are two different problems in trying to answer this question. Together they are called the 'problem of ascertainment'. The first one is that there are an unknown number of undetected crimes and the second major problem is that there is no legal obligation or requirement to report them to any law enforcement agency or even to have a single point within the country to report all cybercrime to.

[24] PCI Security Standards Council LLC, 2008

[25] http://www.gartner.com/DisplayDocument?doc_cd=213836

A good starting point for NCC's regulatory regime could be to develop a Cybersecurity Framework in line with the ITU global security agenda. NCC will also do well to build a national baseline of the various cyber assets; in form of a National Assets Register. As a matter of priority, NCC may want to consider the PCI DSS standard as it applies to the banks, Point of Sales (POS) merchants and the Mobile Money operators. Below is a list of other regulations that NCC may wish to consider to help strengthen Risk management across the country:

- National Assets Register
- Risk Management
- Threat and Vulnerability Assessment
- Business Continuity and Disaster Recovery Plan
- Access Control
- Data Encryption

8. CONCLUSION

Cyber-crime is not a technology problem that can be 'solved'; it is a risk to be managed. The goal of every Cybersecurity and cyber-regulation is therefore universal: to protect; detect; respond to; and recover from cyber-attack, so as to guarantee availability; reliability; safety; confidentiality; integrity; and maintainability of critical services rendered to the citizens. However, this requires an understanding of the nature and magnitude of threats to the infrastructures. Nations therefore take a systematic and pragmatic approach to setting regulations in line with their varied concerns and interests and in such a way as to manage risk that guarantees business profitability and resilience. From the foregoing, a few logical deductions could be made as follows:

- Regulations demands compliance;
- Compliance inspires governance;
- Governance enables sound Business Alignment;
- Alignment brings Profit; and
- Profit means Good Business

Therefore REGULATIONS equal GOOD BUSINESS