

## The Dawning of Information Security Legislations, What Nigerian Corporations Can Do To prepare<sup>1</sup>

**Folajimi Franklin Akinsuyi<sup>2</sup> (LL.B, BL, MSc, LLM)**

Information security relates to the protection of data to ensure its confidentiality, integrity and availability and can be likened to an asset that adds value to an organisation and as such needs to be implemented across the entire organisation environment<sup>3</sup>.

One of the basic misconceptions about information security is that it can be resolved by deploying technology such as automated tools. It must be noted that while technology enhances security it only forms part of a wider picture. Other factors that make up the security pie are issues include employing appropriately skilled resources; development and implementation of policies and procedures, conducting risk assessments, training and educational awareness along with management and legal requirements.

Increasing attention is being brought to the adequacy of information security measures deployed by corporate organisations. This is being driven by increasing number of organised criminals and members of staff successfully breaching corporate organisations network environments.

These incidents have led to a flurry of legislations and regulations, which, mandate appropriate information security measures being enacted. These legislations tend to have global impact due to the fact that while they have been enacted in one country, due to the nature of multinational organisations, we are seeing them influence the way in which these organisations have changed their global information security management practices to ensure they comply with the requirements.

A key feature of these legislations is that while the culprits of security breaches tend to be criminals, these legislations have sections in them that require corporate organisations to adopt measures that will not make it easy for these criminals to be successful in their attempts. The net effect of these legislations is that organisations that have had their systems breached now come under scrutiny and have to prove that they were not partly responsible for the breach due to their lapse or ineffective controls.

Last year in the United States, one of the most significant shifts in the importance of information security and the way in which corporate organisations handle personal information was made when Choicepoint a credit and personal information vendor firm sold personal information to criminals who had set up fraudulent accounts by posing as businesses that run background checks on potential customers. Over

---

<sup>1</sup> First published in the Nigerian Economic Summit Group Economic Indicators March 2006

<sup>2</sup> Franklin F Akinsuyi is the Founding partner of DataLaws an information technology law consultancy based in the United Kingdom. He specialises in Information Technology Contract Negotiations, Information Security Law, Data Protection, Electronic Commerce and Identity Theft. He can be reached at fakinsuyi@datalaws.com

<sup>3</sup> See ISO 17799 first edition 2000-12-01

145,000 accounts were deemed to have been compromised, including those of senators and legislators. It is to be noted that this state of affairs was not detected for over a year. When it came to light, there was uproar and immediate clamour for appropriate legislation to ensure organisations not only develop appropriate security measures, but also that they notify users when their information has been compromised<sup>4</sup>. As a result of the compromise, the Personal Data Privacy and Security Act was enacted on June 29 2005. It is to be noted that Choicepoint has had to pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress<sup>5</sup>

#### Section 404 of the Sarbanes-Oxley Act 2002

This section of the Act has been identified as being responsible for organisations subject to the legislation improving the effectiveness of their internal controls. This includes controls relating to ensuring security and integrity of systems relating to financial reporting systems.

The seventh principle of the 1998 UK Data Protection Act also provides “appropriate levels of security must be implemented in proportion to any harm that may arise due to unlawful processing or unauthorised access and also the nature of data to be protected”.<sup>6</sup>

The Gramm Leach Bliley Act 1999 also makes requirements for appropriate security programme being implemented by organisations<sup>7</sup>

- To comply with the Gramm Leach Bliley Act, all financial institutions must develop a comprehensive written information security program that specifies exactly how their customer data is being protected. The information security program must include the following elements:
- Involve the Board of Directors: The board is responsible for approving and overseeing all aspects of the information security program.
- Identify & Assess Risks: Identify internal and external threats to customer data. Assess the probability that such threats could occur and the potential damage envisioned. Assess how well existing policies, systems and procedures address the identified risks.
- Manage & Control Risks: Develop appropriate security measures to control the identified risks. Examples of such measures include data encryption, employee background checks, intrusion detection, and intrusion response programs.
- Oversee Service Providers: Insure security measures are in place to reduce risks from outside vendors.
- Employee Training: Once an information security program has been designed all employees must receive appropriate training so that they are better able to recognize and respond to security threats.

---

<sup>4</sup> See Choicepoint breach will lead to increased regulation article by Michael Ramussen available at [www.csoonline.com/analyst/report3416.html](http://www.csoonline.com/analyst/report3416.html)

<sup>5</sup> see [www.ftc.gov/opa/2006/01/choicepoint.htm](http://www.ftc.gov/opa/2006/01/choicepoint.htm)

<sup>6</sup> Part 2 section 9 (a & b) Data Protection Act 1998 Sch 1

<sup>7</sup> Gramm-Leach-Bliley Act Public Law 106-102 ss 501 and 505(b), 15 USC ss 6801, 6805 and implementing regulations at 12 C.F.R. Part 30 Appendix B (OCC) 12 C.F.R. Part 208, Appendix D-2.II (A) (Implement a comprehensive written information security program)

- **Test the Program:** The information security program must be tested on a regular basis. Testing should be conducted by independent third parties or staff independent from those who develop and maintain the program.
- **Adjust the Program:** The program should be reviewed on a regular basis and adjusted as needed to meet the changing demands of the institutions business environment. **Report to the Board:** The board should be kept informed on a regular basis regarding all matters pertinent to the program.

Information security breaches are a worldwide problem and have reached a point where it has now been recognised that legislative and regulatory measures are the only way to ensure corporate organisations fulfil their obligations in providing appropriate protection not only of personal information their customers have provided them, but also to reduce the risk of such information being compromised by third parties, internal staff and criminals.

In recent surveys conducted by the National High Tech Crime Unit (NHTCU)<sup>8</sup> the following were identified as the top nine security threats

- Virus attacks
- Unauthorised access to systems
- Theft of confidential information
- System sabotage
- Internal staff abusing internet access
- Financial fraud through deception
- Theft of computer equipment
- Denial of service attacks
- Unauthorised web site modification

The effects of these breaches on organisations affected can run into hundreds and millions of dollars. Indeed it has been estimated that the full global cost of the Sasser worm clean up cost as much as the damage caused by a major hurricane.

In the United States as more states have made it a legal obligation to disclose information security breaches<sup>9</sup>, we have seen that there has been a rise in the number of notifications by organisations that have had their environments compromised informing customers that are likely to be affected by these breaches. This is in stark contrast to their attitude when a breach occurred prior to the legislation being enacted. Before these legislations were put in place, it was not considered wise to notify customers due to the impact it might have on the organisation i.e. loss in confidence, share price devaluation, loss in reputation.

As such, customers only became aware of the event when they checked their accounts finding that money was missing, or being sent a bill for something that they had not paid for, typically in places they had never been. The burden was also placed on the customers to prove that they had not spent the money themselves.

---

<sup>8</sup> [http://www.nhtcu.org/media/documents/publications/8817\\_Survey.pdf](http://www.nhtcu.org/media/documents/publications/8817_Survey.pdf)

<sup>9</sup> Security Breach Notification Laws – State

Security breach notifications<sup>10</sup> now indirectly place the burden on corporate organisations to implement adequate security as well as being proactive in notifying customers so that they are aware and can react swiftly in reducing the effects of their data being compromised.

It is to be noted however that while an information security breach may compromise an organisations environment, along with customer information, it is not in itself an indication that the organisation does not have adequate security or indeed has not done its best to inform those that may be affected by compromise.

In the event that there is an information security breach, the organisation in order to alleviate itself must have show that it took reasonable care in protecting such information from compromise. It is at this point that many organisations fail as they are not able to show that they have taken appropriate steps in implementing appropriate controls on systems:

- where such information is stored,
- when information is transmitted
- when information is being requested
- when information is being retained
- when information is being destroyed

### **Meeting Information Security Legislation Requirements**

Information security is no longer just an issue technology boffin's need to worry about, it has wider reaching implications which executives of organisations need to be on top of.

For large and global organisations, information security goes to the heart of day-to-day activities and as such needs to be given due attention. Indeed with the rising number of legislations being enacted many in-house lawyers are being called upon to advise on information security issues and as such have had to learn more about technology issues in order to provide the advice that will assist their organisations in deploying appropriate strategies.

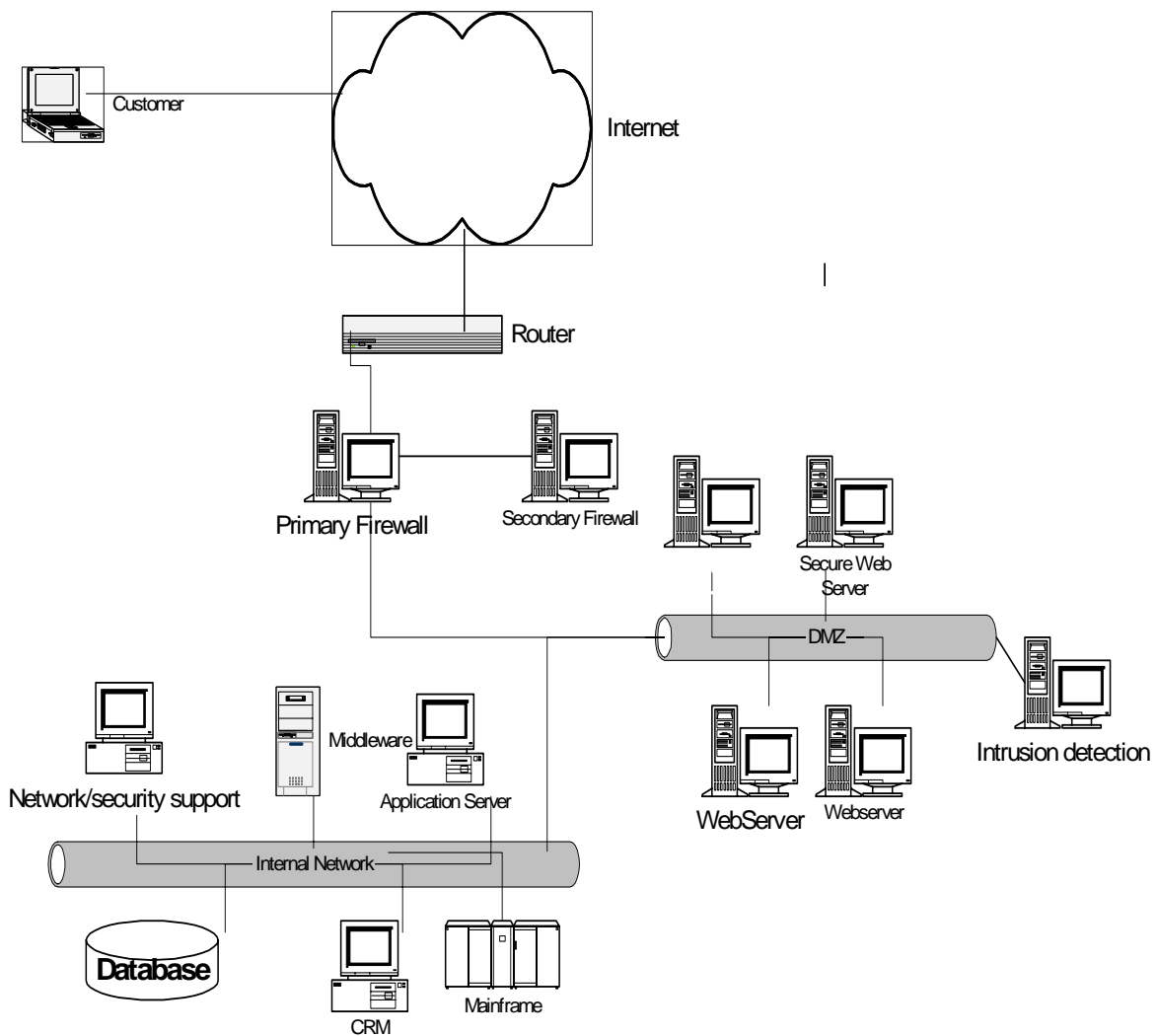
The next three diagrams<sup>11</sup> provide logical incite into how organisations can map their systems to meet legislative information security requirements.

The diagram below shows components of a typical simplified electronic commerce network environment with network systems such as firewalls, webserver, secure webserver, intrusion detection systems, databases, application servers, customer relationship management systems and mainframes.

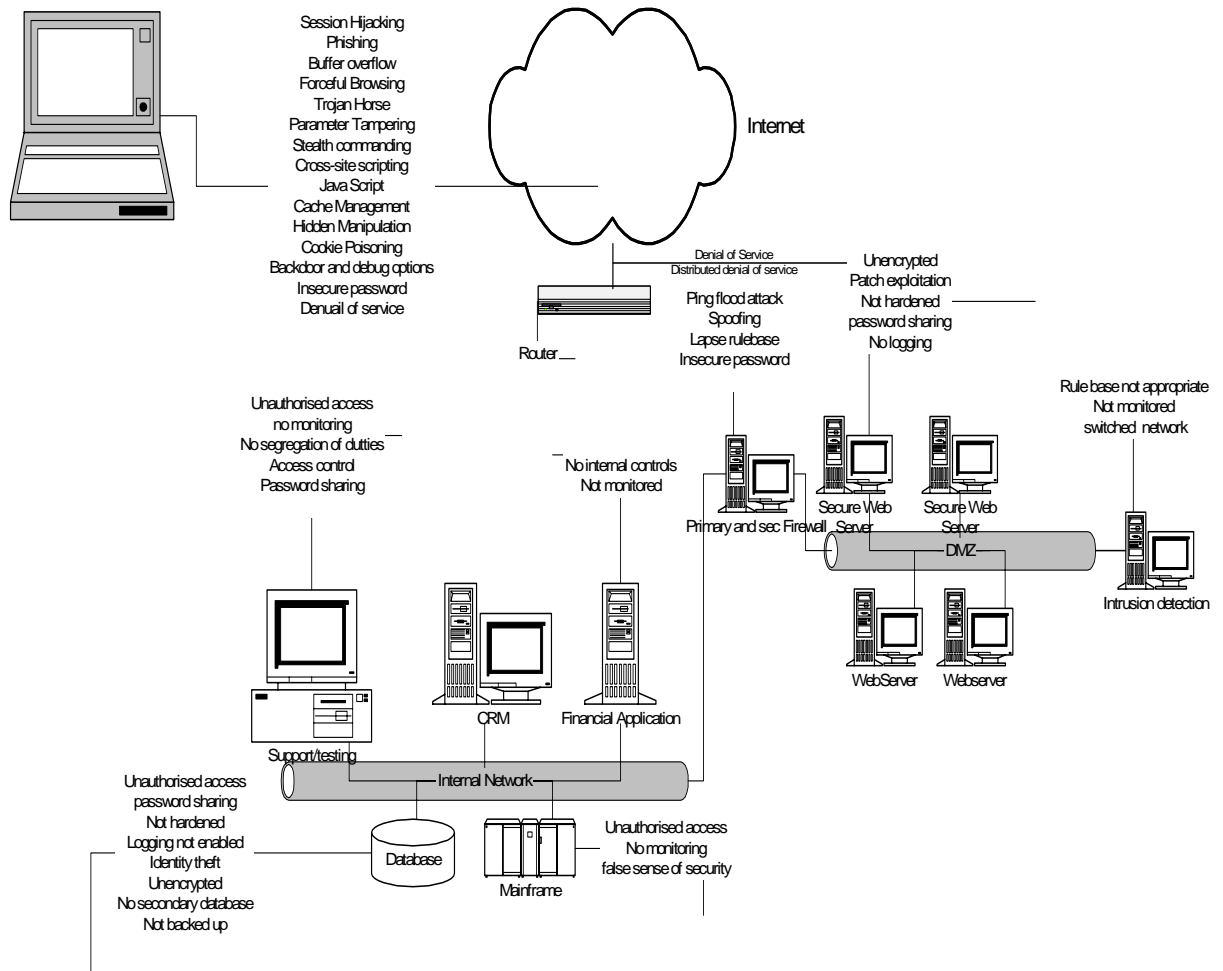
---

Security Breach Notification Laws – State  
State Citation  
Arkansas Ark. Code Ann. § 4-110-101 *et seq.*  
California Cal. Civ. Code § 1798.82  
Connecticut 2005 Conn. Acts 148  
Delaware De. Code Ann. tit. 6, 12B-101 *et seq.*

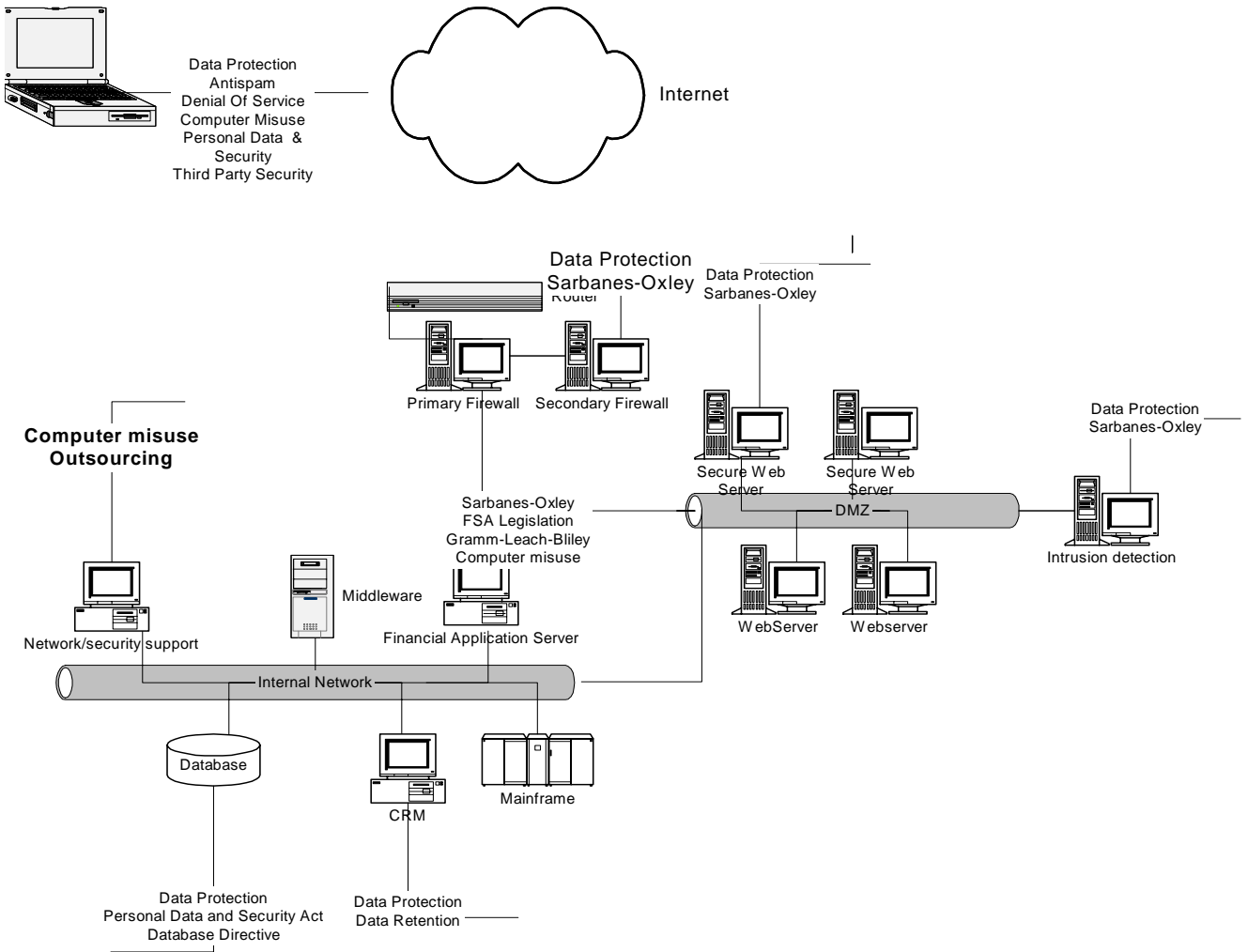
<sup>11</sup> Taken from “Harnessing technology and law to combat crime in Ghana” written by Franklin Akinsuyi and presented by DataLaws at the British High Commission in Ghana November 2005



The diagram below shows a sampling of information security threat types and where in an electronic commerce network information security breaches can occur.



The diagram below identifies information security legislation and what systems their relevant sections can affect.



The diagrams above show how legislation can influence logical mapping of information security requirements.

In order to effectively attain information security compliance, organisations should as a first step look to industry standard information security guidelines. Adherence to industry standard practices is way of showing that due care has been taken in reducing the risk of successful breaches.

Implementing and obtaining certification of ISO 17799 - (recently replaced by ISO 27001) information security management standard can act as evidence to prove an organisation is taking information security seriously.

What is ISO 17799, and how do organisations adapt their current practices to meet it?

ISO 17799 is an information security management code of practice. It includes a number of sections, covering a wide range of security issues.

Listed below is an outline these sections and their objectives:

#### ***1. System Policy***

This section deals with management direction and support for information security. It is to be noted that in drafting security policies, it will typically involve a number of key persons input before senior management signs it off. The drafting should involve input from Human Resources, as abuse of policies will include terms relating to disciplinary actions. In the determination of a security policy lawyers will also need to be called upon to review sections in relation to their enforceability and legality.

#### ***2. Security Organisation***

The objective of this section is two pronged:

- a) The management of information security within the organisation
- b) The maintenance of the security of information and processing facilities in relation to external parties such as third parties, and partners.

#### ***3. Asset Management***

The purpose of this section is to:

Firstly achieve and maintain appropriate protection of the organisations assets, and secondly ensure that information receives an appropriate level of protection  
This typically will consist of ensuring all assets are accounted for and classified according to sensitivity levels in order to ensure only authorised persons can access the asset.

#### ***4. Personnel Security***

This section identifies measures an organisation should take in order to ensure that employees, contractors, third parties etc are suitable for the roles they have been employed or contracted to perform. It also involves making these persons aware of their responsibilities towards staff, the organisation and third parties.

### ***5. Physical Security***

This section provides insight into measures that may be required to prevent unauthorised physical access, interference and damage to the organisations information and physical building. Its objective also includes preventing theft, loss and damage to physical assets along with preventing interruption to the organisations activities.

### ***6. Communications and Operations Management***

This section provides guidelines on how to manage communications and operations It has 11 subsections, which are listed below:

- a) Ensure the secure operation of information processing facilities
- b) Maintain the appropriate level of information security and service delivery, aligned with 3rd party agreements
- c) Minimise the risk of systems failures
- d) Protect the integrity of information and software
- e) Maintain the availability and integrity of information and processing facilities
- f) Ensure the protection of information in networks and of the supporting infrastructure
- g) Prevent unauthorised disclosure, modification, removal or destruction of assets.
- h) Prevent unauthorised disruption of business activities.
- i) Maintain the security of information and/or software exchanged internally and externally.
- j) Ensure the security of e-commerce services
- k) Detect unauthorised information processing activities

### ***7. Access Control***

One of the most important sections in my view, access control forms the bedrock of information security. This section provides guidelines on how to effectively:

- a) Control access to organisations information
- b) Ensure users are authorised to have access to information
- c) Prevent unauthorised access to information systems
- d) Prevent unauthorised user access and compromise of information and processing environments
- e) Prevent unauthorised access to network services
- f) Prevent unauthorised access to operating systems
- g) Prevent unauthorised access to information within applications
- h) Ensure information security in relation to mobile computing and teleworking environments

### ***8. Information Systems Development and Maintenance***

This section of the standard provides guidelines in relation to the development, change management and implementation into the production environment. Its objectives are to:

- a) Ensure that security is an integral part of information systems, this includes
- b) Prevent loss, errors or unauthorised modification/use of information within applications
- c) Protect the confidentiality, integrity or authenticity of information via cryptography
- d) Ensure the security of system files
- e) Maintain the security of application system information and software
- f) Reduce/manage risks resulting from exploitation of known vulnerabilities

### ***9. Business Continuity Management***

This section of the standard provides incite into what an organisation needs to do to ensure it can operate when there is a major disaster.

### ***10. Compliance***

In line with the theme of this article is the standards section on compliance, which provides guidelines on avoiding breaching legislation, regulations or contractual obligations.

Its two other objectives are to ensure systems comply with the organisations internal policies and standards and also maximise the effectiveness of and minimise associated interference from and to the systems audit process

It must be mentioned that prior to placing security measures on systems any organisation in attempting to reduce exposure to common security threats must identify where its main risks lie. This can be achieved by conducting a risk assessment. A risk assessment entails an organisation identifying where reasonably foreseeable threats to its environment may come from. This will include both internal source threats and external source threats.

The assessment will also involve analysing how likely the threat will occur

Estimating the damage that may occur and costs to clear up the damage

On completion of the assessment, there may be situations where the organisation may have to accept the risk in the form of a waiver.

The object of conducting a risk assessment is to ensure the right resources are utilised in proportion to the risk the organisation may face

### **What does this mean to for Nigeria and Nigerian corporations?**

As has been stated above, security breach notification legislation has been quite effective in making corporations own up to breaches where personal information has been involved. It has also made organisations implement more stringent information security management practices.

As electronic commerce grows in Nigeria for example, financial service organisations will need to adopt the benefits of technology by offering secure services online.

In order to meet global legislative standards, Nigeria will need to enact legislation that makes it mandatory for organisations to adopt appropriate information security measures commensurate with the risks that may accrue to the organisation in question<sup>12</sup>.

Those responsible for drafting Nigeria's Cybercrime/ Information security laws can ensure that they include sections that make it mandatory risk assessment to be carried out by financial organisations offering Internet related services.

This can be similar to the guidelines of the Federal Financial Institutes Examinations Council<sup>13</sup> which stipulates that: "The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by an organisations internet banking systems. The risk should be evaluated in the light of the type of

---

<sup>12</sup> See Franklin F Akinsuyi "Requirement for rapid development of a legal standard information security framework for Nigeria"

<sup>13</sup> See <http://www.ffiec.gov/>

customer (e.g. retail or commercial) the customer transactional capabilities (i.e. bill payment, wire transfer, loan origination); the sensitivity of the customers information being communicated to both the institution and the customer; the ease of using the communication method; and the volume of transactions<sup>14</sup>.” This guidance also goes on to state that the level of authentication used in a particular transaction should be appropriate to the level of risk in that application<sup>15</sup>.

When Nigeria implements its Cyber/Information security legislations, many organisations will need to adapt to the requirements.

While information security legislations are developing, it is to be noted that information security standards remain for the most part static. This being the case, rather than try to forecast how to meet future legislative requirements, Nigerian companies can sidestep the need to understand the legislative requirements by adopting the requirements of information security standards. These standards provide industry recognised guidelines on how to implement and manage information security. As has been explained above, ISO 17799 (27001) is an ideal starting point towards the road for implementing effective information security measures.

#### Concluding

To conclude, it has been mentioned in the body of this article that there has been a rise in information security breaches, in order to counter rising system breaches to corporate organisations, new information security legislations have been enacted in Europe and North America. Many of these legislations make it mandatory for organisations to implement adequate information security controls commensurate to the risks that may accrue to systems within their environments. While there are no adequate information security legislations in Nigeria at present, corporate organisations can implement appropriate information security controls on their systems, such that by the time information security/Cyber security legislations come into effect, they will already be in a position to meet these requirements. Following industry guidelines not only allows for legislative compliance, it also reduces the threat of successful information security breaches and inspires confidence in investors.

---

<sup>14</sup> FFIEC Guidance p.3

<sup>15</sup> FFIEC Guidance p.3