

Requirement for Rapid Development of a Legal Standard Information Security Framework for Nigeria¹

Franklin Folajimi Akinsuyi² (LL.B, BL, MSc, LLM)

The rapid development and availability of computers, coupled with the advent of the Internet have led to major changes in the way information can be utilised.

It has been established that information has value and as such all data owners ranging from governments, financial institutions to military establishments have recognised the need to deploy technology to assist them ensure sensitive information is accessed only by authorised persons.

Recent media coverage of information security breaches have shown that all forms of organisations are vulnerable to systems being compromised where adequate measures are not put in place.

Information security breaches can come from two sources, internal breaches that involve members of staff, along with external security breaches, which are carried out by third parties.

While it is widely recognised that internal breaches are more rampant and attributed to consist of an estimated 75% of security breaches as identified in a survey of security breaches conducted by the FBI (A computer crime survey³ which identified that out of 488 respondents, 77% stated that the likely source of attack on proprietary information was disgruntled employees)

Despite the above findings, external security breaches are given more exposure; this can be attributed to a number of reasons.

In the first instance, the shock value of an external entity being able to break into network system conjures up images of a shady individual in a dark room plying his computer skills to steal money or confidential information from systems is high. It must also be noted that as information technology advances, information relating to breaking into computer systems have become freely available to persons interested in the art of computer hacking and cracking. As an illustration a UK teenager was prosecuted for successfully gaining access to the Pentagon network⁴. What is all the more surprising about this breach is that the individual concerned did so from the comfort of his bedroom.

¹ Published in Nigerian Economic Summit Group Economic Indicators July-September 2005 Volume 11 No 3

² 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

³ See page 8 CSI/FBI Computer Crime and Security Survey available upon request from Computer Security Institute www.gocsi.com/press/200020407.html

⁴ see <http://www.kimsoft.com/korea/hack-16.htm>

Another reason why more attention has been given to external security breaches is the fact that successful internal security breaches are not usually announced by organisations falling victim. Many are aware that revealing this information may have negative effects on their reputation, which may lead to share price devaluations for private companies.

When external breaches occur the targeted organisation can be seen as the victim of unauthorised access attempts events, which on the face of it may seem as if they have no control.

Internal security breaches on the other hand put the organisations processes, procedures and policies under scrutiny; they may need to prove that their standards fulfil compliance and regulatory requirements. As such organisations tend to keep such information under wraps rather than involve the media or tell their shareholders.

It is the aspect of ensuring organisations whether public or private maintain adequate information security standards that needs to be looked at in further detail.

It is to be noted in the past, many organisations, which suffered security breaches whether internal or external were not under the spotlight to prove they had adequate measures in place.

The increasing development of electronic commerce and Cybercrime especially the rise of identity theft have led to numerous legislations being enacted in Europe and America which make it mandatory for organisations to implement adequate information security techniques.

In the United States Legislation such as the 2001 Gramm-Leach-Bliley Act have made it mandatory for commercial organisations to implement adequate information security measures to protect customer information.

Legislation has also been passed in California to the effect that businesses are now obliged to disclose any breach of the security of their systems to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person⁵.

Section 404 of the Sarbanes-Oxley Act of 2002 has also had an impact on the way in which organisations apply internal controls on financial reporting systems.

⁵ California Civil Code Sections 1798.29 and 1798.82 – 1798.84

The rise in identity theft has also had an impact on legislation as can be illustrated with the recent high profile security breaches at Choicepoint and Lexisnexis⁶ both of which have been hit by large scale identity theft of personal information stored on their databases. It is to be noted that these particular breaches have led to a clamour for stringent legislation. As a result of the uproar and lapse security measures, US senators are introducing the Personal Data and Security Act 2005.

In Europe, laws relating to communications security can be found in legislations such as the EU Privacy and Communications Directive, Article 4 (1) of which stipulates that adequate security measures must be implemented by organisations that process personal information. This law is transposed into national legislations of Member States.

In the UK this can be illustrated by section 5 of the 2003 Privacy and Electronic Communications (EC Directive) Regulations, which states that providers of public electronic communications service should take appropriate technical and organisational measures to safeguard the security of that service.⁷ The Regulations define appropriate measures as being those that are taken in relation to technological developments and the cost of implementing it in proportion to the risks of safeguards⁸.

The seventh principle of the 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”.⁹

In Nigeria, it is to be noted that the government and commercial organisations are embarking on a number of electronic commerce projects. In implementing these projects it is imperative that information security is understood and applied at the beginning rather than after the event, a common mistake made by many.

The government and indeed the legislature can play a part in defining minimum information security requirements to be adopted by establishments handling personal and financial information. In order to adopt the right approach they need to ensure they understand what risks can accrue and the measures which may be used to counter or reduce the risk of information being accessed by unauthorised persons.

The government is also embarking on the development of the Cybercrime Act, in order to implement this effectively, an understanding of Information Security standards such as ISO 15408¹⁰ and ISO 17799¹¹ needs to be undertaken. This will

⁶ See Security breach at LexisNexis now appears larger: Article by Heather Timmons and Tom Zeller JR NewYork Times April 13, 2005

⁷ Section 5 (1) Privacy and Electronic Communications (EC Directive) Regulations 2003

⁸ Section 5 (4) Privacy and Electronic Communications (EC Directive) Regulations 2003

⁹ Part 2 section 9 (a & b) Data Protection Act 1998 Sch 1

¹⁰ ISO 15408 (The Common Criteria for IT Security Evaluations)

¹¹ ISO 17799 (Standard for Information Security Management)

allow for appropriate legislative coverage and inclusion of sections, which will ensure cogent issues are addressed.

Nigeria stands to gain enormously from adopting an information security and data protection framework. By enacting appropriate information security legislation, Nigeria will be able to take a step in the bridging the gap between technology and law.

We have seen that the adoption of technology can facilitate investments from foreign countries thus aiding income of indigenes. This can be well illustrated in the Asian Pacific continents where numerous foreign companies have in their quest for competitiveness and reduction of costs invested heavily in the development of call centres.

The potential for this model to be adopted in Nigeria is highly feasible. This can be buttressed by the fact that many indigenes speak very good English are highly educated and are able to grasp the use of technology in commercial environments

One of the major issues preventing this from occurring is a lack of existing legislation. For instance as mentioned above, the European Data Protection Directive stipulates that personal data should not be transferred to countries outside the European Economic Area unless such countries have similar Data Protection Legislation.

It is issues such as these that excludes Nigeria from benefiting from offshore outsourcing, and the development of technology infrastructures that come with it.

The detriment of not implementing such legislations is that Nigeria will be left behind in advances in technology, thus creating a greater digital divide with the rest of the world.

Synergy between information security and law:

In recent years, the rise in threats and vulnerabilities that can lead to computer systems being compromised, has led to corporations implementing information security management systems to protect themselves from malicious attacks against their environments. These threats have also led to private individuals who log on to the Internet from their home computers purchasing personal firewalls to guard against external probes to their internet sessions.

It is issues such as these that have made information security one of the fastest growing areas of information technology along with information security consultants being able to command higher than industry average fees for their services.

A common misconception about information security is that all that is required is to remove threats, is the deployment of technology systems. It is to be noted that while technology is used to mitigate the risk of compromise, it is just one aspect of a well thought out and effective information security solution.

Other aspects of the information security jigsaw include:

- the creation of processes, policies and procedures which will be used to define what is to be done in the day to day management of information security operations
- Identification of who is responsible for escalating and dealing with information security incidents
- What to do and how to react in the event that there is an information security breach.

As has been stated earlier information security is one of the fastest growing sectors of the information technology industry. One of the reasons for this is that with every new technology come risks of new threats. For instance, in the mid nineties, organisations wishing to communicate more effectively deployed email systems, they however discovered that without appropriate anti-virus protection, their email systems could easily be compromised, aligned to this was also the risk of unauthorised sending of emails with company information enclosed in attachments. This led to the demand and deployment of content checking tools to scan and quarantine suspicious emails prior to them either being sent out or entering the corporate environment.

In the late-nineties many financial institutions implemented on-line banking systems. These organisations discovered that their systems could easily be compromised if they did not deploy perimeter devices such as firewalls, intrusion detection systems, network scanning and database protection tools. As a result, Firewalls, intrusion detection, network scanning and database protection tools became the most widely demanded information security devices.

In the new millennium, what one can see is that while firewalls and intrusion detection systems are still necessary and content checking tools along with anti-virus software is still in high demand, there has been widespread growth in website portals being run by governments that have realised that it is easier, cheaper, convenient and more reliable for customers to use services which require processing via forms such as vehicle registration and e-conveyancing online. Many electronic commerce websites have also sprung up due to small and medium sized companies taking advantage of the commercial benefits offered by the Internet.

The information security risks that these types of websites are susceptible to, calls for the deployment of application security scanning tools that can be used to identify weaknesses in the code on such websites. As such the demand for application scanning software has also seen large growth.

In recent years the high levels of information security breaches have not gone unnoticed by the legislative arms of many developed countries. Indeed a number of legislations have been enacted in response to the effects these successful information security breaches have on persons that may be affected by them.

In the United States, many states have implemented legislation that makes it mandatory for organisations that have had their environments breached to notify their customers of such events.¹²

¹² See [California Security Breach Information Act, Senate Bill 1386](#), California Code of Regulations, Title 10, Sections 2689.12 to 2689.20

Other legislations have made it mandatory for organisations to implement information technology measures such that they can be used to protect personal information stored on systems under their control.¹³

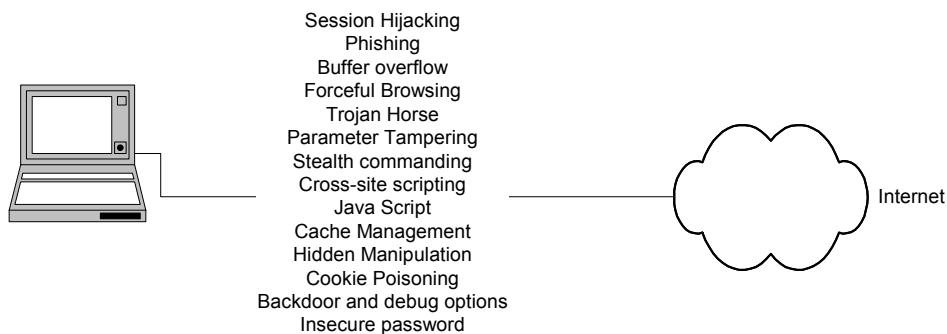
It can be stated that while the law is struggling to catch up with fast changing technological advances, it is beginning to hold its own in the area of information security.

An easily identifiable synergy between information security and law can be illustrated when using the Internet.

At the point where an individual logs onto the Internet wishing for instance to purchase an item online, the information and information security issues become identifiable.

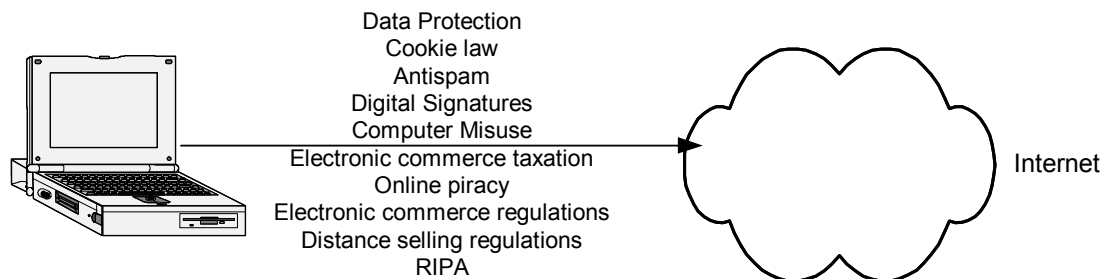
The information security risks that can be accrued to a user trying to gain access to a website from their home can be illustrated in diagram A below:

Diagram A: Information Security Risks:



Legislation that the user is subject to while trying to access the website is as follows and is also illustrated in the network diagram B below:

Diagram B: Information Technology Legislation:



¹³ See Section 5 (1) Privacy and Electronic Communications (EC Directive) Regulations 2003

The above diagrams show how and what point the user is simultaneously affected by legislative issues and information security risks as soon as they begin an Internet session.

It is at this point that we need to look at the Nigerian environment and identify how we can harness legislation to deal with information security risks that individuals who sign up to services provided by commercial websites such as the e-government portal, online banking and other commercial websites will be exposed to.

Nigerian Legal Standard Information Security Framework

Nigeria is in the throes of developing its cyber security laws, in order for these laws to be effective, associated risks to users, organisations and indeed the government must be identified prior to such legislation being enacted.

The reasons why these risks need to be identified become apparent when one considers the effects of fast changing technology developments. If the risks are not identified, there lies the possibility that the legislation will be outdated as soon as it comes into effect and as such will not be effective in combating the issues it has been put in place to curtail.

It is therefore necessary when defining cybersecurity legislations that they fall under the ambit of an information security law framework which can easily be adapted to meet the changing technology developments.

In implementing the information security law framework, considerations need to be made for future technological changes in the way and manner people, organisations and governments will utilise technology.

Future forecasting on issues relating to electronic banking, mobile and fixed line communications, electronic commerce, data protection, and identity theft can serve as parameters against which sections of these legislations can be worded such that the legislation keeps abreast of technological changes.

The question is what issues are foreseeable and how do we ensure the legislation is effective?

Let us take Internet Banking services as an example:

Nigerian financial institutions are developing Internet based services for their customers. This involves the collection, processing, retention and deletion of personal information.

Personal information has value, when it is processed by organisations in the provision of their services it needs to be protected. As part of the legal information security framework, data protection needs to be a subset. The data protection aspect of the framework can be used to govern what and how an organisation can legally process customer's information.

It is widely accepted that identity theft has risen sharply¹⁴; financial institutions that contemplate offering internet banking services will need to conduct risk assessments both on their internal and web facing environments to ensure they have configured systems and scanned their environments prior to offering their services to the public.

Implementing a data protection regime can allow for appropriate regulation of how personal data is collected and managed. This will include ensuring that data collected is appropriate, not excessive, only used for the purpose for which it is collected and not kept longer than is necessary.

Examples of Data Protection Breach:

As has been mentioned, the development of technology has led to more convenient methods of carrying out daily routines; indeed, many activities which in the past required physical presence before a purchase could be made of a product now only need the supply of personal details. The down side of this is that while it has led to faster means of communicating and development of business, there is especially with the advent of the Internet a rise in “identity theft”¹⁵.

In the United States and Europe the proliferation of business activity has led to a number of organisations being established to broker personal information. This has led to a number of underhanded means of collecting personal information in what appear to be promotional information leaflets only for this information to be collated and then sold to marketing companies. It is this type of activity that has led to the call and development of data protection laws leading to stiff penalties for organisations that breach them. Indeed, under the UK 1998 Data Protection Act it is an offence for a person, knowingly or recklessly, without the consent of the data controller, to obtain personal data¹⁶.

To buttress this point further an individual named Alistair Fraser, trading as Solent Credit Control¹⁷, recently pleaded guilty to offences of unlawfully obtaining and selling personal information in breach of the Data Protection Act 1998. Mr Fraser had obtained the personal information of certain individuals by deception from the Department for Works and Pensions. He then sold the information to third parties. He was found guilty and fined. A feature of this case is the fact that it was brought to court by the Information Commissioner, thus showing that the Commissioner is prepared to use enforcement powers to combat and discover agencies that illegally obtain and sell personal information¹⁸.

In the United States organisations that breach the provisions of data protection legislations relating to privacy of information are severely punished on conviction as

¹⁴ See Combating Identity theft: Article by F F Akinsuyi available at www.datalaws.com/html/articles.htm

¹⁵ For the purpose of this essay “Identity theft” occurs when a person or group of people obtain and use someone else’s name, credit card number, social security number or other personal information without that persons consent with the intent of using such information to commit fraud or other crime

¹⁶Section 55 (1&3) Data Protection Act 1998

¹⁷ See www.csa-uk.com/news-facts-press_index/newsletters/autumn202002.pdf page2

¹⁸ Section 60 (1) Data Protection Act 1998

can be illustrated where recently in United States of America (for the Federal Trade Commission) v. Hershey Foods Corporation¹⁹: In this case, Mrs. Fields Cookies and Hershey Foods Corporation each agreed to settle Federal Trade Commission charges that their Web sites violated the Children's Online Privacy Protection Act (COPPA)²⁰ Rule by collecting personal information from children without first obtaining the proper parental consent. Mrs. Fields are to pay civil penalties of \$100,000 while Hershey will pay civil penalties of \$85,000. The separate settlements also bar the companies from violating the Rule in the future and represent the biggest COPPA penalties awarded to date. The COPPA Rule applies to operators of commercial Web sites and online services directed to children under the age of 13 and to general audience Web sites and online services that knowingly collect personal information from children under 13. Amongst other things, the Rule requires that Web site operators obtain verifiable consent from a parent or guardian before they collect personal information from children²¹.

There are a number of other risks that can accrue to customer's information when they carry out their transactions online and also when the data is being processed and stored internally within these companies. These risks include internal and external breaches to customer information. Some of which have been highlighted above.

With these risks in mind, one can understand why it is necessary when developing legislation that appropriately skilled individuals both in the legislative and information security fields are called upon to share their ideas and experience prior to putting pen to paper. (It is not how quickly the legislation is drafted, but how effective it will be when enacted!)

In order to develop appropriate information security legislation to ensure financial institutions safeguard the confidentiality and integrity of customer's information, it is imperative that the legislation makes it mandatory for these institutions to implement up to date industry standard technologies that can mitigate against the risks that can lead to customer data being compromised. This should include specifying that policies, procedures and processes be implemented and managed according to industry-based standards (Legislation similar to section 404 of the Sarbanes-Oxley Act can cater for these issues).

In the event that there is a breach of security and customer information is compromised, the legislation must also mete out appropriate sanctions for organisations that are found not to have implemented such measures or are deemed to have been negligent in the management of such systems.

The legislation must also include these institutions making customers aware when there is a breach that may have a negative impact on the information that has been affected (as is seen in the United States of America).

It must also be mentioned that while obligations are placed on organisations, there must also be a reciprocal placement on users/individuals. Legislation must also cater

¹⁹ see www.ftc.gov/opa/2003/02/hersheyfield.htm

²⁰ 15 U.S.C 6501-6505

²¹ U.S.C 6502 b (1) A ii

for misuse of computer systems by individuals. Computer misuse legislation, which defines and provides appropriate sanctions for illegal activities when using a computer system, can also be made part of this framework.

Internet banking is beset by a number of legislative issues especially where information security is concerned. These legislations will not only affect electronic and mobile commerce environments, they can also be used to stipulate how other commercial entities manage personal information.

With this identified a blanket information security framework rather than sectoral legislations can be devised to regulate these activities. The benefit of this approach is that it serves as a one-stop shop to identify all information security legislative requirements to which organisations and individuals can reference.

To Conclude:

There is undoubtedly going to be a rise in information technology development within the next five years in the Nigerian environment. New services ranging from Internet banking, mobile commerce and online services are earmarked to go live.

With increasing successful information security risks that can accrue when providing and gaining access to these services, it is necessary that legislative frameworks, which regulate all players, be enacted.

One of these frameworks will need to be centred on information security. This framework will need to cater for all risks and vulnerabilities that may be exploited both on the part of organisations providing these services along with individuals who access systems.

The Framework should as a minimum consist of the following types of legislation:

- Information Security
- Data Protection
- Data Retention
- Computer Misuse
- Lawful interception
- Identity Theft

A key issue to making this process successful is for both technical and legal persons with adequate experience coming together to define what is technically and legally feasible when defining what the legislation is to consist of.

This will allow for legislation that has been enacted to be comprehensive, enforceable and up to date.

Copyright Franklin F. Akinsuyi (2005)