Building Global Competitiveness through Information Security Education

Jide Awe

Building Global Competitiveness through Information Security Education

Globally competitive nations are able to key into the benefits of the knowledge economy. Nigeria and other African nations need to compete better in order to improve the quality of life of their citizens. New opportunities emerging daily are due to innovations in technology and the adoption of new ideas. Nations are all competing for global market share. Global competition is about the quest for overall national prosperity – job and wealth creation, developing strategies that facilitate sustainable economic growth[1].

Globally competitive environments are investment magnets that attract jobs, creating investments and entrepreneurial opportunities. To compete globally, the people of Nigeria must have the competence and agility to meet the changing demands of the technology-driven economy. The ability to put brainpower to use is critical to ensuring competitiveness. Quality of human capital is therefore, a major factor in building global competitiveness. Specifically, a competitive economy is one that produces high quality human capital in the critical specialty areas of the global market. Information security is a niche area that Nigeria should consider.

Framework for Global Competitiveness through Information Security Education

To analyse Information security opportunities and education, let us consider the following key areas:

- Key issues in Information Security
- Key Issues for Information Security Education
- Information Security Career Opportunities
- Strategies for Growth in Information Security Education

Information Security

The rapid rate of change in technology developments means technology has always outpaced security. More individuals and organisations than ever before are getting digitally connected[2]. Increase in digital consumption comes with attendant risks. How safe are we, how protected are we as we embrace the digital revolution? Information is the key resource in today's age and the ways we use information have changed - how we work, interact and do business. Information is the key resource, but how secure is this resource? How well are information and associated systems protected from unauthorised access, use, disclosure, disruption, modification or destruction? The security of information is a fundamental requirement for sustainable growth through technology. Nigeria wants the benefits of the Information revolution, but what are the strings attached? Understanding the fundamentals of Information and Communication Technology (ICT) and its implications for society and business requires a thorough appreciation of Information security. In fact, today, Information security and its core principles encompassing integrity, confidentiality, privacy, availability and assurance, is a major concern for all countries – developing and developed.

Our networked world means that knowledge today is local, national and global. This state of affairs obviously has implications for security. Information protection isn't just your network, your organisation or corporate espionage but now includes global linkages such as terrorism. Interestingly, security functions are often primarily seen as a cost centre, when in fact, a true and deep understanding will reveal that effective security is a key enabler of development. For example, no investor will put money in an unsafe environment. Safety promotes confidence and growth. It certainly makes no sense to invest millions in ICT infrastructure and yet be careless with protection of such assets. Investing is all about risk taking, but investing in information security means risks are calculated. It is imperative to manage risks in an informed manner. Ignorance is no excuse in the knowledge world. More interactions and business conducted electronically means more benefits will stream in and so will the associated risks.

Global Information Security Scenario

The new world has emerged – the world of constant change – new technologies, new opportunities, and new threats. Greater access to technology and information results in better, higher quality digital linkages for the good and bad. Tapping into the online world is a necessity. But how secure is learning, business and interaction in the knowledge economy? Hackers, spam, hostile software, online attacks, worms and identity theft are just a few of the dangers encountered as people exploit Internet and web based opportunities. Online bandits, web fraudsters and digital masqueraders thrive in the same world of net entrepreneurs, online megastores and e-corporations; the electronic marketplace or the digital jungle?

> *Investing is all about risk taking, but investing in information security means risks are calculated.*

Information security has become a major concern for all. Readily available hacking tools have increased the risk of hostile hackers breaking into networks and computer systems. Intrusion attempts are growing in number and complexity. According to Robert S. Mueller III, Director, Federal Bureau of Investigation (FBI)'s statement[3] before the United States Senate Judiciary Committee in March 25, 2009, addressing cyber security has become one of his country's top three national security priorities, and annual estimated loss to financial institutions in responding to cyber attacks exceeds $200 million in the United States alone.

As far back as 2004, the United Kingdom (UK) Hi-Tech Crime Unit's survey found that 83% of UK companies had been the victims of computer crime. Initial digital threats were pranks. The objectives were usually to irritate victims, to prove a point, to spread a message or impress and boast or to shock with exhibitionistic displays of programming skills. However, the threat on Net has moved from digital pranksters to hardened criminals. The "bad guys" have taken over. Organised crime has gone digital. In the words of Peter Szor[4], Author *The Art of Computer Virus Research and Defense*,"The new attackers are serious fraudsters involved in organised crime. Malicious computer programs are used to steal personal information that includes social security numbers, bank account information, passwords, and so on. Attackers are highly motivated by money, and I believe the reason for the sudden increase in computer worm attacks is due to this".

Information security is serious business. Organisations that deploy ICT must address security. Local businesses that think and act global will have to deal with these security concerns. Information security is a priority for individuals and businesses that desire to take advantage of the global new economy opportunities. Security threats will not disappear overnight. Information security is no longer an afterthought. Information security is a critical business enabler. Information is critical to global processes and transactions. However, global online bandits are here for the long haul. This along with the growing and massive demand for information and ICT enabled products and services are driving up the demand for security in the information society.

The Information Security Challenge

How prepared is Nigeria to meet the challenge? By building confidence and security into the use of information and communication technologies (ICTs), Nigeria and its people are better positioned to tap into the benefits of Information security. But why is this not happening. Let's look at some of the causes:

The digital divide[5] - The digital divide is still a problem for Nigeria and most African countries – the majority of the African populace, especially those living in the rural areas are still "offline". Even in the urban areas, many are still grappling to come to terms with new digital realities. Quite a few continue to attempt to ride the dead horse of the old economy. To others, ICT isn't an enabler; there is no connection between ICT deployment and business strategy. Open hostility may even be displayed to ICT related developments. ICT is seen by such people as a "bottomless pit" into which money is poured.

Lack of understanding of what Information security means is a major societal challenge. Significant numbers of people learning, interacting and working online are unaware of the threats and the significance of the threats. It's strange but people still fall victim to Automatic Teller Machine (ATM), recharge card and the "Bill Gates is giving away all his money" scams. Access and consumption is the main focus of many. The demand for digital access and inclusion is justified, as Nigeria cannot afford to be left behind in the digital revolution. But how many know that the same Personal Computer (PC) that helps you to get the job done faster can also be a welcoming mat for danger?

Lack of interest in education and training

Lack of understanding is compounded by lack of interest in security education. Security is a serious issue but demand for security expertise is surprisingly weak. It is amazing that in the corporate environment, there is a belief that "crime happens to someone else". There is an "it can't happen to me" mentality. Security education is not regarded as a priority. Instead, interest and demand in the ICT education is for user and the core professional skills. Which is more important - how to provide an ICT facilitated service or how to secure such a service? What is the value of the unprotected database masterpiece? How dependable is a network that does not work due to incessant attacks? Poor demand for security education reflects the low level of security awareness in the environment. The erroneous belief is that security education is a luxury and not a necessity. "It should be common sense". "Security skills can be picked up by professionals as they progress in the field". Developing security expertise should never be reduced to gambling or "trial and error" experimentation.

Direction of governments is unclear

Although, Nigeria and several African governments have developed security and ICT policies[6], implementation is a major challenge. "Paper policies" – clearer policy direction is required. And how realistic are such policies? How much has been invested in terms of time, education, personnel, etc? What are the priorities? Is deployment effective? Is content relevant? How committed is leadership? How effectively are resources mobilised and deployed? Are the policies government "shows" or are other stakeholders involved? How well integrated and prioritised are the policies within national development programs?

In addition, most measures taken on Information security are reactive in nature, e.g. pursuing the 'Yahoo boys'. Government must realise that Policies on Information security are not simply a buzzword for making the right noise. Quality will take a back seat where issues such as planning, research, monitoring, human resource development and statistics are not given priority attention. Haphazard half measures don't work. There is need for better focus and coordination of efforts rather than playing to the gallery.

Low confidence exhibited in electronic business (e-business) structures

The poor attention paid to Information security has affected the growth of e-business in Nigeria. It isn't enough for banks and merchants to churn out e-business products and services; is the environment right? Does the environment breed confidence in online transactions – locally and globally? In the deployment of e-banking (ATM, Internet, etc) what have the banks and other stakeholders in the e-payment industry done to promote an environment of confidence and trust. It isn't enough to spend on marketing and promotion; investors and key stakeholders – local and foreign – will not take e-business serious in an insecure environment. Within Nigeria, debit cards have gained tremendous acceptance for cash related business transactions. However, Nigeria's e-payment infrastructure needs to be enhanced to enable increased participation in global online business. The activities of Internet fraudsters are however, impeding efforts to build global confidence in Nigeria's e-payment structures.

Law Enforcement/Security/Intelligence Agencies Gap

Information security involves combating crime. A major challenge, however, is that of empowering law enforcement in the digital era, the ICT infrastructure of law enforcement requires massive improvement. The "analogue" days of law enforcement are over; crime fighters must be equipped with critical and relevant skills for knowledge economy security and intelligence. Security and intelligence activities today cover more than the physical and the tangible. Information security covers not just ICT knowledge but ICT enabled intelligence. There is need to equip the police with skills to deal with the threats associated with Information infrastructure, products and services enabled by ICT. Loud noise on cyber crime is simply beating around the bush; there is no need for drama and theatrics. We simply cannot police what we don't understand. Information security remains in the realm of ideas – and is ineffective – without the support of law enforcement. Information protection requires legal enforcement otherwise, cyber crime will thrive. Law enforcement agents must have the skills, know-how and necessary insight to fight knowledge economy crime. It means knowing how to encourage whistle blowing, identify threats, protect assets and arrest offenders. Security operatives (in the private and public sectors) and interested members of the legal profession who want to take advantage of knowledge economy opportunities may also find it useful to develop skills in Information security.

The poor attention paid to Information security has affected the growth of e-business in Nigeria.

The Information Security Expertise Need

Information protection is critical in the knowledge economy. Businesses need expertise for protecting the value and ongoing usability of assets and integrity, and continuity of operations. This involves identifying threats and then choosing the most effective set of tools to combat them. Security expertise is required to ensure protection from threats - internal and external, as well as the intentional and the unintentional. According to 7th Annual Trends in Information Security survey[7] for the Computing Technology Industry Association (CompTIA), 'human error is the primary cause of most severe security breaches.' There is little doubt that security education improves information security.

Surveys continually indicate that human action contributes more to security failures than technological weaknesses. Do we understand the nature of the enemy? The enemy isn't technology; the enemy isn't outside, it isn't simply a software or anti-virus issue.

Security education needs can be divided into two categories: user education needs and specialist education needs

Information Security Awareness for the Non-Tech (user, client, manager)

"Unintentional security breaches by non-IT staff, cost companies thousands of dollars in lost productivity and business downtime. This demonstrates a need for more employee trainings and deeper knowledge of technology functions". - A CompTIA Analysis of IT Security and the Workforce[8]. People need to be educated - to understand security threats and vulnerabilities. Users and managers shouldn't be content with using ICT; they need critical knowledge and insights into the latest technology, tools and strategies in Information security. What are the myths and reality? What works, what hinders Information security? The alternative is to become a victim and become a home or launching pad for Cyber attacks. The hackers are prepared and ready. Are the users?

Secure operations mean fewer losses, more productivity and a very real advantage. Unfortunately, a significant number prefer to save money rather than secure their business; it is important to see security as a business enabler. How would an e-enabled corporation quantify the costs associated by disruptions caused by hackers? There is need for a clear understanding of the use and misuse of ICT and related facilities.

Information security isn't a technology issue. In fact, security is everybody's business. There must be security awareness at all levels from executives and everyday users. They must all speak the same language. Individuals and organisations need to know that their security is only as strong as their weakest link. Acquiring and installing the latest information security technologies makes no sense in an environment where behavioural safeguards are absent. Do people take the proper steps when incidents occur? Are users aware of the need to use the right type of passwords? If Information security is regarded as a priority, it will be seen as a necessity rather than a burden. Users in particular must get beyond the 'I just want to get my job done' approach when using ICT, by being proactive about security. Danger is ever present and everybody (users, professionals, business managers and policy makers) needs to adopt good security habits. But there is need to strike the right balance. Too much security can be unproductive and stifling.

Users and managers shouldn't be content with using ICT; they need critical knowledge and insights into the latest technology, tools and strategies in Information security.

Based on the need to develop Information security awareness and capacity in Africa, the International Conference[9] on Computer Security and Cyber crime was organised for the very first time in Africa, in March 2006. The conference objectives were to: develop a framework for computer and internet security in Africa; establish guidelines for cyber-laws in Africa; promote civil liberties in internet use; highlight critical security threats, issues and technologies affecting information and computing infrastructure; learn how to protect your organisation's computing environment and critical infrastructure; gain the insight and practical knowledge to protect and defend technology and related infrastructures.

At the end of the International Conference on Computer Security and Cybercrime in Africa, participants resolved to establish the African Information Security Association[10] (AISA) to facilitate and promote information security in Africa. AISA aims to present users, professionals, managers and policy makers with the opportunity to be part of current and future Information security developments in Africa.

Information Security Specialist (more knowledge, more secure and efficient)

The job/work of the Information security specialist is to keep out the 'bad guys' and help secure information assets and network from unauthorised access, e-mail attacks and malicious code viruses.

It requires technical ICT competence as well as mastery of issues that include: digital certificates, authentication, encryption keys, firewalls and intrusion detection, business availability, disaster recovery planning, social engineering and business knowledge. Because of information security's impact and close relationship with crime and society, security professionals need to have a solid grasp of ethical and legal issues.

The ethical hacking approach – 'trying to catch a thief, by thinking like a thief' – is an approach adopted by many security professionals. How do cybercriminals think? What are the weaknesses? Why and what do they attack? What is in the hackers mind?

Information security professional needs knowledge tools to close the expertise gap. They often learn from experience and develop expertise by investing in relevant training and certification programs. Furthermore, Information security requires a forward thinking, proactive mindset. Lifelong learning is imperative in such a dynamic, fast changing field.

Information Security Certifications and Career

The significant advantage of certification is the emphasis on work-driven industry and societal needs. Quality certifications are based on learning, current risks, threats, technologies, global best practices and standards.

Some of the recognised information security certifications[11] include Security+ developed by the Computing Technology Industry Association (CompTIA), the Certified Information Systems Auditor (CISA) program sponsored by the Information Systems Audit and Control Association (ISACA), Certified Information Systems Security.

Professional (CISSP) certification from International Information System Security Certification Consortium, Inc (ISC)[12], Cisco Certified Security Professional (CCSP) certification from Cisco systems and Microsoft Certified System Engineer (MCSE) Security certification for Microsoft corporation. Certifications only validate technical competence. Careers in information security in addition, require lifelong commitment and interest. An information security professional guards the whole perimeter, while the attacker needs only one point of entry. Information security is no joke. Unlike conventional 'old school, brick-and-mortar' security assign-ments, it deals with both the tangible (physical protection) and the intangible (software, virtual networks, information protection). Because of the impact of known threats, security is a popular area these days in ICT knowledge and career circles. However, popularity alone is inadequate for making sound career decisions. Protecting information isn't a job for quick fixers. It requires commitment and the ability to shoulder immense responsibilities relating to ethics, technical, legal, business, people and constant learning.

There is a broad range of jobs and entrepreneur opportunities in Information security for students, professionals and managers in ICT, law enforcement, Defense, Military, Security and the legal profession. In particular, demand for information security expertise is constant and growing in Education, Independent Consulting, Security outsourcing and the development of security products and services. For example, in the application development space, secure development processes is becoming mandatory and it is no wonder that the demand for security outsourcing is on the increase.

Strategies for Growth in Information Security Education

> *The ethical hacking approach – 'trying to catch a thief, by thinking like a thief' – is an approach adopted by many security professionals.*

Growing Information security education in our environment requires a multidimensional approach. First, the environment and strategies should stimulate the development and retention of human excellence in Information security. This should go hand in hand with public information security awareness interventions. Domestic market opportunities should be developed and promoted to drive demand for jobs, entrepreneurs, while improving information security for organisations.

In addition to the awareness campaign, conscious efforts should be made to identify, highlight and pursue global niche opportunities for Information security expertise. The IT curriculum at all levels in the national education and training system should be updated to integrate Information security.

Other Issues Affecting Global Competitiveness (not a cure-all)

The challenges mentioned earlier should show that Information security on its own is not the only requirement for global competitiveness. The hostile environment is in fact, a major hindrance. The high cost of business setup, multiple taxation pricing, as well as inefficient and corrupt business practices cannot help

Nigeria compete globally. Issues relating to quality of infrastructure are critical. Global competitiveness will be difficult without attending to the problem of power supply as well as low level of ICT penetration.

The environment, to a large extent determines the quality of competitiveness. The right environment must have effective policies to address Information security, ICT for development and the development of the domestic market. Information security should be an integral component of the national ICT and economic policies.

Government, security agencies, private sector must be proactive in complementing the efforts of AISA. There is no one-man army in information security. And waiting for major problems/violations is irresponsible. Establishing legal and regulatory frameworks to support e-business, ICT and ICT enabled activity is therefore, imperative. Legal infrastructure is required to practically address law enforcement, consumer protection, Intellectual property rights, Cybercrime, electronic contracts, data protection and other aspects of information security. Towards this end, Nigeria's House of Representatives held a public hearing on draft legislation for Cyber Security and the Information Protection Agency[12] in July, 2009.

Summary and Conclusions

Lack of support and direction hampers competitiveness. How can we take advantage of new economy opportunities in such a hostile environment? Should we just give up and go home? Here are suggestions on the way forward. The action points require the active involvement of all stakeholders, including Government, academia, industry, private training organisations, NGOs and students.

1. There is need for more debate, dialogue, networking, and action on information security education in Africa. AISA and the international conference mentioned earlier are important initiatives. Government should understand and define the national value proposition offered by Information security. Information security expertise is high on the global value chain. Nigeria and other African countries should exploit it as an opportunity to create wealth, jobs and drive sustainable economic growth

2. Speed up efforts to establish legal and regulatory frameworks to support e-business, ICT and ICT enabled activity.

3. Individuals and organisations interested in Information security should seize the initiative by investing in Information security education. It is possible to turn the challenge into opportunity.

4. The gender digital gap reduces the impact of the knowledge economy. In developing and promoting Information security education, the lack of sufficient participation by women in science, mathematics, IT, and technology, must be addressed. Programmes should be designed to support female enrolment.

5. The education system should be transformed to incorporate and recognise global best practices, standards, the culture of entrepreneurship and lifelong learning in the area of Information security. Creative options and incentives should be adopted to make security education attractive.

6. Information Security education for Law Enforcement/ Intelligence personnel must be taken as a priority. Modern ICT infrastructure should be deployed to support law Enforcement and Intelligence agencies.

7. Innovation and research must be promoted in Information security. Beyond promoting information security in the work place, there is need to develop research and local content development strategies. Statistics should be captured to effectively monitor and measure the impact of Information security. Data collected should be used to identify gaps and for planning purposes.

I end by paraphrasing the *ILO*[13], "Education and training is the root and branch of global competitiveness". epr

Jide Awe is the Founder/CEO of Jidaw.com (http://www.jidaw.com)

[1] Global Competitiveness Network of the World Economic Forum http://www.weforum.org/en/initiatives/gcp/index.htm

[2] International Telecommunication Union ITU http://www.itu.int/net/about/global-communications.aspx

[3] Federal Bureau of Investigation (FBI) Congressional Testimony, March 25, 2009 http://www.fbi.gov/congress/congress09/mueller032509.htm

[4] Computer Virus Research and Defense http://www.peterszor.com/

[5] Awe Real Independence, Nigeria, ICT for Development http://www.jidaw.com/nigeria/independence_ict_nigeria.html

[6] ICT Policy in Nigeria http://www.jidaw.com/policy.html

[7] CompTIA's 7th Annual Trends in Information Security http://www.comptia.org/research/security.aspx

[8] CompTIA Analysis of IT Security and the Workforce http://www.comptia.org/news/pressreleases/09-03-10/Lack_of_End_User_Training_is_a_Large_and_Growing_Threat_to_IT_Security_CompTIA_Study_Finds.aspx

[9] International Conference on Computer Security and Cybercrime http://www.jidaw.com/security2006/index.html

[10] African Information Security Association (AISA) http://www.jidaw.com/security/aisa/aisa.html

[11] Information Security certifications http://www.jidaw.com/certarticles/securitycerts.html

[12] Cyber Security and the Information Protection Agency Nigeria http://www.jidaw.com/security/aisa/public_hearing_nigeria_draft_bill_cyber_security.html

[13] ILO's World Employment Report http://ilo-mirror.library.cornell.edu/public/english/bureau/inf/pkits/wer98/wer98ch2.htm