INFORMATION SECURITY AWARENESS: A KEY TO THE SUCCESS OF ORGANIZATIONS IN THE 21ST CENTURY

Christian C. Njoku

Abstract

Digital Information security is one of the sensitive areas of concern discussed in organizations especially at the senior management level in leading organizations. As the world becomes a global village, most organizations today rely on technology in order to achieve competitive advantage as one of their major objectives. However, information security has been one of the major challenges for conducting successful business on global scale. Modern organizations can no longer confine themselves with the technical aspect of information security. For these organizations to achieve their business objectives, they need to take a proactive stance and look beyond the technical aspects of information security. This paper takes a critical look at the concept of information security, causes of information security breaches and the types of information security breaches. It also discussed the concept of information security awareness, the importance of awareness and how to raise awareness. Useful recommendations were made.

An organization's people, information, operations, and systems are critical assets. Protecting the safety, confidentiality, integrity, and availability of these assets is essential to maintaining profitability, compliance, public image, and a competitive edge. Security awareness provides the greatest return on investment and has the greatest positive impact on a company's security.

The rapid and dramatic advances in information technology (IT) in recent years have without question, made positive impact in the world. At the same time however, it has created significant and unique risks to most organizations' operations. With the invention of computers, information has moved from paper-based format to an electronic bit-based format. As the world embraces technology and gets connected, so the door to threats and information leaks open wider. Internet connectivity is on the increase as more devices such as computers and mobile phones are hooked to the net on daily basis. Also, the increase in connectivity of these devices brings more people to the knowledge of computer usage. With the rate at which the world is going, virtually all organizations and private establishments are getting connected to the internet so as to meet up with the standards of international business. Information is stored, shared and disseminated faster through computer networks thereby, increasing transactions. However, little thought is given to the security of this information. This is a major problem as the most valuable asset a company or organization possesses is her information. (Zorz, 2008). Computer security has in turn, become much more important as all levels of government utilize information systems security measures to avoid data tampering, fraud, disruptions in critical operations and inappropriate disclosure of sensitive information. Such use of computer security is essential in minimizing the risk of malicious attacks from individuals and groups. The major reason for the increase in security threat is the excess dependence on the computer as a data processing and decision-making tool in sensitive functional areas.

Electronic information is also essential to the achievement of government organizational objectives. Its reliability, integrity and availability are of significant concerns in most organizations. The use of computer networks especially the Internet is changing the way government and other organizations carry out business. The benefits of this have been enormous and vast amounts of

information are now literally readily available. These interconnections also cause noteworthy risks to computer systems and the infrastructures they support.

Lainhart, (2011) outlined three major categories of threats which occur as a result of increase in data, devices and connections. They are: external threats, internal threats and compliance requirements. He noticed that external attacks have passed from individuals working independently to attacks, that have become more coordinated. This is usually launched by groups ranging from criminal enterprises to organized collections of hackers. The attackers are not only seeking profit but sometimes, for prestige and espionage. These attackers target more important organizational assets which may include customer databases, intellectual property and possibly physical assets driven by information systems. These may also cause very serious financial consequences.

On the other hand, internal threats or breaches may not be carried out by external threats but by insiders. Internal threats range from careless behavior and administrative mistakes such as giving away passwords to others, losing back-up plates, laptops or storage devices, willfully releasing sensitive information and deliberate actions taken by discontented employees.

On the issue of compliance, Organizations should have a glance at security and compliance as an opportunity and not just a necessity of little business value. Non-compliance can be a threat to any organization, but if properly taken care of, it's a priceless prospect which can be utilized to embed IT security throughout the entire organization. Compliance objectives should, as a matter of fact, involve senior management in the issue of IT security; it's no longer an IT problem but a company initiative, and serves as a good beginning to greater coalition and teamwork across management.

What to comply with should include: Data Protection Act 1998 which is a Legislation concerned with handling personal data which includes employee and customer information, Regulatory of Investigatory Powers Act 2000 , a Legislation about the acquisition and disclosure of information, The Financial Services Authority (FSA),a regulation specific to finance & retail or companies that take payment card transactions and ISO27001, a standard and specification for an Information Security Management System (ISMS). (Nui solutions, 2011).

Information Security

This can be seen as the protection given to a computerized information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources which include hardware, software, firmware, information/data and telecommunications. It also means a technique developed to safeguard information and information systems stored in computers.

Computer security is of increasing importance to all levels of government for minimizing the risk of malicious attacks from individuals and groups. These risks include the fraudulent loss or misuse of organization's resources, unauthorized access to release of sensitive information such as tax and medical records, disruption of critical operations through virus or hacker attacks and modification or destruction of data. Computers are faced with threats ranging from natural disasters (fire, flood, earthquake and hurricanes), to human threats (discontented employees, hackers, virtual theft and physical theft, human error and hardware damage). Also, the data and software on the computer need to be protected from accidental or intentional loss and tampering.

Information security breaches may occur in various ways such as: loss of information held by agencies or organizations, loss through stolen laptops and loss through backup devices such as external hard disks and other storage devices which contain such sensitive information. It could also be through disposal of computer hard drives and other storage media without erasing contents. Again, if an employee of a particular organization mistakenly discloses or releases information to the wrong

person, for instance, sending mail to the address or releasing organization's information for selfish interest or gain to one who wants to use it against the organization. Databases containing an organization's information can be hacked into or illegally accessed by individuals outside of the agency or organization. (Commonwealth of Australia, 2008).

Another non-technical threat worthy of mentioning is social engineering. This uses human interaction to break security procedures. This might involve gaining the confidence of employees with access to secure information; tricking them into thinking there is a legitimate request to access secure information; physical observation and eavesdropping on people at work. Social engineering preys on the fact that people are unable to keep up with rapid advance of technology and little awareness of the value of information to which they have access (Tassabehji, 2013).

The most common type of attack is from viruses and malware followed by hacking or unauthorized access to networks resulting in vandalism of websites and theft of equipment (mainly laptops). Denial-of-service attacks are less frequent relative to viruses, with financial fraud and theft of information being the lowest kind of security breach experienced. However, it should be noted that the latter two types of breaches would be hard to detect in the short term and the impact of the previous attacks would have an indirect effect on the information stored. (Tassabehji, 2013).

Harms caused by Information Security Breaches

Where there is security breach of information in organizations, there is always a threat to physical safety, financial loss of business opportunities. There is also humiliation, damage to reputation or relationships. Apart from the results mentioned above, there is loss of trust in the organization and loss of assets. There are also serious regulatory penalties and legal proceedings. These are some of the harms any organization may have as a result of information security breach, hence, the need for information security awareness.

Information Security Awareness

Information is undeniably the 'blood' of any organization. It is a valuable business asset in today's IT-driven world. Computer systems and networks link every department and connect people with countless suppliers, printers and markets. (Hinston, 2008). Access to high-quality, complete, accurate and up-to-date information makes managerial decision-making relatively easy by reducing the margin for error. Steichen (2008) suggested that people in the organization should be aware of the need for security of information systems and networks and what they can do to enhance security. Information security awareness refers to sharing information with, educating, and training users about risks to data, especially on its confidentiality, integrity, or availability of data, and about knowing what to do to protect it.

Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. People in the organization should understand that security failures may considerably harm systems and network under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. The people in the organization especially the IT personnel should be aware of the configuration of, and available updates for, their system. They should maintain good practices that they can implement to enhance security and the needs of other participants.

The basic truth is that security is about people not really technology. Therefore, protecting and enhancing the value of information is so crucial and it is only synonymous with profit making. The major cause of security breaches/human error has been the person behind the computer and this has not been properly addressed therefore he continues to be primary source of the organizations' problems. Therefore, to really create a security culture, however, awareness has to permeate throughout all organizational levels. A good way to make people understand security better is to make

the value of information being protected clear by shedding light on the risks and consequences associated with losing or compromising that information.

It is against this backdrop that it was observed that technical security controls are strong but they have to be correctly specified, designed, developed, implemented, configured, used and maintained. Simply put, security-aware managers, staff and IT professionals make better use of technical security controls. This point was buttressed by Contos (2006) as he observed that "for years people have been investing in preventive measures – firewalls, and other technologies of that nature but there hasn't been much focus on the core". The insider threats are easily perpetrated because the countermeasures that in place to counter external attacker does not hinder them (the insider). Therefore, expenditure on security technologies such as firewalls, antivirus should be matched by spending on security processes including of course security awareness. Formal security policies, no matter how carefully they are written, are of little value unless employees know about them, understand their obligations and actively comply. In other words, if employees do not understand their roles in the security plan, investing time and money into securing the organization and its customers can be undermined (Hinson, 2008).

Making computer system users aware of their security responsibilities and teaching them correct practices help users change their behavior. It also supports individual accountability which is one of the most important ways to improve computer security. Without knowing the necessary security measures, users cannot be truly accountable for their actions. This idea was supported by Dorian (2008) who revealed that awareness and training are capable of bridging the gap between the technical controls to be effective, senior management needs to support awareness and training within the organization. He believed that the twenty minutes it takes an employee to review an awareness presentation may be, the difference between a secure organization and a multi-million dollar breach of security. The concept of educating employees on how to protect data will never be completely replaced by technical security controls.

Hinson (2010) stated that information security controls will certainly improve the organization's profitability by reducing both the number and the extent of information security breaches as well as reducing both the direct and indirect costs.

Khan (2010) asserted that one of the best ways of creating information security awareness is for all employees within the organization to be given appropriate training on information security policy and the organization's security prospect in line with their functional roles. As an example, the corporate internet usage policy should be communicated, read, understood and accepted by all employee within the organization. In addition, a role-specific- policy such as the enterprise software management policy, should be scoped to include relevant employee, for example the IT systems department. Furthermore, it is important for organizations to monitor the spreading of policies and procedures through employee attestation. This will provide a priceless input into policy enforcement and education processes.

In addition, Khan (2010) revealed that people are the weakest link when it comes to organizational security. This goes on to say that it does not really matter how much an organization spends on securing organization's information rather, the attention given to the people behind the IT facilities matters much. Therefore, the organization's information security program will be an ineffective exercises if an adequate level of information security awareness is not also implemented. Generally speaking, almost all organizations are required to educate their personnels on policy and security awareness.

Furthermore, to implement a formidable information security awareness, information security policies should address the communication, reporting, escalation and resolution of information

security events and weaknesses. System auditing, availability statistics and performance metrics provide vital information to assist in the evaluation and monitoring of incidents and potential vulnerabilities. This data can then be utilized for work plan validation or even forensics analysis following an incident or serious breach. The information security incident management procedure should be explicitly documented and all employees, contractors and third-parties should be educated in its requirements and their associated responsibilities. (Khan, 2010).

Moreover, detailed and reliable information security controls reduce the organization's overall risk profile. Good information security builds management's confidence and trust, allowing the organization to press ahead with business opportunities that might otherwise be too risky to contemplate. Part of this arises from better knowledge of the extent of security breaches that occur consistently. Reporting information about actual and potential security breaches to management is a sign of a mature information security framework.

The Importance of Information Security Awareness

The best way to achieve a considerable and enduring progress in information security is not by bringing in more technical solutions to the problem, it is by raising awareness, training and educating everyone who interacts with computer networks, systems, and information in the basics of information security. In the words of Hinson (2008), the following points are the importance of Information security awareness programs:

1. It helps employees recognize and respond accordingly to real and potential security concerns
2. It provides fresh and up-to-date information to keep staff current on new risks and how to go about them.
3. Employees, contractors and business partners are made to be aware that the data on their computers and their mobile devices (PDAs, thumb drives, smart phones) are important and vulnerable.
4. It informs the people about information security risks and controls in a general sense and provides more specific information and guidance where necessary.
5. It motivates people to behave in a more security-conscious manner.

Security awareness programs will also improve morale by providing information that is personally useful to a staff, such as how to avoid scams, fraud, phishing and identity theft. Furthermore, it will save money as it will reduce the number of security breaches. This is because the sooner breach is identified, the lower the costs of addressing it. Information security awareness programs provide savings through coordination and measurement of all security awareness, training and educational activities while reducing duplication of efforts.

Information security awareness gives organizations a competitive advantage, protect and enhance organization's reputation and brand. This is important as it tells the customers that the organization cares about protecting their information. It reduces the potential for lawsuits against organization by demonstrating a corporate concern for security and a process for ensuring that the workforce will provide adequate protection for information assets entrusted to its care.

How to raise Awareness of Information Security

For a successful awareness to be raised, organizations must see it as a long term investment. Raising awareness includes personalizing risks for managers, showing them how vulnerabilities could affect them as individuals. Increasingly, for awareness to be effective, it should have design phase, developmental phase, implementation phase, evaluation phase and this must be specific, realistic and measurable. (Steichen, 2008). In addition, Hinson (2008) suggested that for effective security awareness to hold, there must be an extent to which staff understand the importance of information security, the level of security required by the organization and their individual security

responsibilities. The staff should be able to act accordingly across the organization and should be endorsed by top management.

A planned and coordinated awareness program, according to Hinson (2008) helps secure the organization's information assets by bringing a dissimilar range of security awareness, training and educational measures under management control. It can also be planned by providing a management and measurement framework, and a variety of communication techniques and tools. Facilitating disciplinary or legal action against those who fail to comply with their information security obligations is also another planned awareness program. Other planned and coordinated awareness program includes improving the consistency of application of information security controls.

Furthermore, there should be a target group with similar interest and priorities and the presenter should understand the audience especially their level of understanding on the issue at hand. The following practices have been adjudged by Steichen (2008) as best for raising security awareness:

1. Major stakeholders should be scouted for and be made to participate in decision making, planning, implementation and evaluation.
2. A comprehensive objective should be established for the change endpoint after consulting with major stakeholders.
3. There should be a proper description of responsibilities, roles and accountabilities.
4. There should be need to handle risks, also barriers to change should be taken care of.
5. There should be room for adjustments in approaches to go with different stakeholders needs.

Conclusion

It is said and believed that risk and business have always been together, however today, new information security risks are coming up with strange challenges for firms and governments alike. Apart from terrorist groups using information tools and developing cyber capabilities, foreign governments are involved in serious espionage, and criminal syndicates are setting up well-planned cybercrime operations. Organizations are not left out as they are facing new generation threats that are often difficult to detect, and it's nearly impossible to assess their long-term consequences.

Considering the rate at which the world is becoming a global village through technology, it becomes a difficult thing for anybody or organization to think that their information is 100 percent safe. A lot is been done to at least, fight the menace; several technical methods are in use such as cryptography, the use of several IT devices, etc but this paper is of the opinion that creating awareness, which is a non-technical method will do more than the technical methods. Information security awareness gets everybody in the organization involved as it educates them on the need to be information security conscious and it makes everyone in the organization take responsibility. Furthermore, security awareness could go a long way in changing the behavior of employees in an organization. Therefore, it is less important how a security organization is structured, the main issue is that the organization has the right people to implement security checks successfully.

Recommendation

The following recommendations are hereby proffered if organizations must win the war on information security:

1). Organizations must develop, communicate, roll-out and publish an all-inclusive set of approved organizational information security policies. These policies must be read, understood and acknowledged by all employee within the organization.

2). There must be a clear alliance of the organization's information security activities with strategic business and technology activities. This is because a gap between the information security activities and strategic business requirements may potentially result in a variety of adverse impacts across the organization.

3). There should be an analysis of the current state of organizational information security, and a clear definition of a realistic target state.

4). Executives and senior level management need to be aware of, engaged in, and supportive of security issues, strategies, and policies. Senior management involvement is essential because many high-level decisions – outsourcing, joint ventures, etc have security implications that senior management often doesn't consider.

5). Information security awareness program must be understood and acknowledged by the organization's personnel and should be communicated using clear terms and language.

References

Brian Contos (2006): quoted Brian Contos, author of *Energy at the Water Cooler*.

Hinson, G. (2008): *The true value of Information Security Awareness*. Retrieved from http://www.noticeboard.com/html/why_awareness.html on 15/08/2012.

James Dorrian (2008): quoted from *the US Computer Security Act and FISMA*, plus James Dorrian's security awareness piece in INSECURE Magazine vol. 17.

An Babiak (2006): quoted from a *CompTIA security survey report*.

Johnson, M.E. & Goetz, E. (2007): *Embedding Information Security into the Organization*. Published by the IEEE Computer Society. www.computer.org/security/.

Khan, R. (2010): *Practical Approaches to Organizational Information Security Management*. SANS Institute Reading Room.

Lainhart, J. &Robinson, S. (2011): *Managing threats in the digital age*. IBM Institute for Business Value. Produced in the United States America.

Steichen, P. (2008): *Advanced Security Methodologies – Awareness raising*.

Peltier, T.R. (2005): *Implementing an Information Security Awareness Program*. Security Management Practices. United State of America.

Security Awareness: A Sound Business Strategy. Retrieved from http://www.nativeintelligence.com/niprograms/whyaware.asp on 20/01/2013.

Zorz, M. (2008): *Network and Information Security in Europe Today*. INSECURE Magazine. www.insecuremag.com.

Benefits of Information Security Awareness. Retrieved from http://nativeintelligence.com/ni-programs/ni-benefits.asp on 07/01/2013.

Commonwealth of Australia (2008): *Guide to handling personal information security breaches* (Archived). Retrieved from http://www.privacy.gov.au /materials/types/ guidelines/view /6478 on 28/02/2013.

Compliance & security: Navigating its complexities (2011): Niu Solutions. Retrieved from http://www.niusolutions.com/media/downloads/White%20Papers/Compliance%20-and-%20Security% 20Whitepaper.pdf on 02/02/2014.

IT Security and Compliance: They can Live Happily Ever After.Retrieved from http://www. dimensiondata.com /Global/Downloadable% 20Documents/IT% 20Security%20and %20Compliance%20Opinion%20Piece.pdf on 02/02/2014.