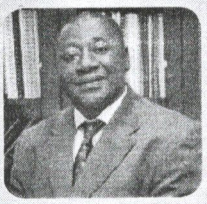
Implementing an information security strategy for universities

ICT WORLD

with

Nana Prof. Osei K. Darkwa



GENERALLY, information security (sometimes shortened to InfoSec) has been defined as the practice of preventing unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

It refers to protecting these elements and related processes in terms of confidentiality, integrity and availability (CIA) of information while maintaining a focus on efficient policy implementation without hampering organisation productivity.

Others view it as the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

According to Pipkin, it is the process of protecting the intellectual property of an organisation. And McDermott and Geer regard it as a risk management discipline, whose job is to manage the cost of information risk to the business.

Information security is regarded as a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organisational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

The source of the information may take any form, electronic or physical.

It may take the form of application security (dealing with software vulnerabilities in web and mobile applications and application programming interfaces); cloud security (focuses on building and hosting secure applications in cloud environments); encrypting data (such as the use of digital signatures in cryptography to validate the authenticity of data); infrastructure security (that deals with the protection of internal and extranet networks); and incident response to monitor for and investigate potentially malicious behavior.

THREATS

Information security threats come in many different forms. Some of the most common threats today are software attacks (such as viruses, worms, phishing, Trojan horses, etc.), theft of intellectual property, identity theft (e.g., acting as someone else to obtain that person's personal information), theft of equipment or information, sabotage (e.g., destruction of an organisation's website in an attempt to cause loss of confidence), and information extortion (e.g., theft of an organisation's information or property in an attempt to receive a payment in exchange for returning the information to the owner).

Regardless of the form it takes, the primary objective of information security is to protect an organisation's information assets from unauthorised uses, breaches, and disclosure.

Universities have become an essential part of the fabric of our civilisation. Society requires universities since they play a crucial role in our search for new knowledge and our civic life.

They are becoming amazingly complex organisations and their scope for compliance regulations is wider and more complex than other industries.

Today's universities offer services ranging from student registration, online billing, academic transcript services, accommodation, food services and others to their students and other stakeholders, and manage significant data processing operations.

Research documents that today's universities have become a complicated maze of physical campuses, online learning, students, faculty, alumni, and research partners from both the public and private sectors. They store huge data about students, parents, alumni, faculty, and staff.

When students graduate, most institutional policies require that data is kept for a considerable period of time.

And these processes and interactions create a large and evolving threat surface that makes institutions a target for cyber attack. Most universities recognise the threats their institutions are facing in a technological world.

They are a frequent target for cyber attacks because of the sensitive data their IT systems often house. The proliferation of connected devices on campuses makes it harder to secure and protect all potential entry points.

SECURITY

Thus, managing security risks responsibly builds a platform which will enable them to seize these opportunities and embrace the future.

Safeguarding information and information systems is essential to preserving the ability of universities to perform their mission and meet its responsibilities to students, faculty, staff, and the citizens whom it serves.

Most universities have implemented information security policies to help safeguard their information resources from accidental or intentional damage and data from alteration or theft.

The purpose of most of this policy is to ensure the protection of information resources from accidental or intentional access or damage while also preserving and nurturing the open, information-sharing requirements of academic culture.

How do we protect university data. Fact is, there is no easy solution to this, given the large and diverse campus population of users who need to be educated on potential dangers, but who don't always realise the issues or take them seriously.

Successful higher education cybersecurity requires communication between the IT department and institutional leaders, so they can be more effective in preventing attacks and bouncing back after an incident occurs.

An Information Security strategy should be created and considered in such a way that it is built into an organisation's overall strategy.

If the security strategy is not helping the institution meet its goals of educating students, conducting research and facilitating community outreach, then it is irrelevant and will not meet its goals.

The need to work with departments and faculties across the entire university spectrum is crucial to ensure proportionate and robust IT solutions are in place supporting the overall university information security strategy.

Policies to secure remote access of the institution's data need to be put in place. The development of an information asset register allows the institution to know the state of its IT assets.

Also, the need to develop a training and awareness programmes for the university community is crucial, given the rapidly changing nature of today's technology.

Information security is a global challenge. Thus, international collaboration is needed to deal with the problem. While these suggestions will not guarantee the security of IT systems, it will go a long way to reduce the impact of cyber theft.

The writer is the president, African Virtual Campus