**WHY IS THEZITH MORE CONCERN ABOUT IT EMPLOYEES?**

So basically a start would be more concern about it employees because human are more vulnerable, we are the most vulnerable people, therefore it has to be concerned about it employee’s, thou you might have all the security measures in check and make it well known, the employees are still vulnerable to a lot of attacks but awareness helps reduce the percentage.

Cyber security risk can happen at a work place, but a large percentage can be avoided by changing the employee’s behaviour and making awareness in the company.

Attacks like ransomware, social engineering, phishing, and many more expose the company to higher threats using the employees, a strong awareness on opening of email should be thoroughly checked before accessing and trusting social networks, this could be taken lightly by most employees, leaving the company at risk, phishing and social engineering mostly occur on social media, most employees just assume social sites are safe, just because of personal interaction.

All start-up companies would be very concerned about it data, it should be that they ensure they notify IT departments on when employees are terminated, therefore all usernames and password should immediately be shutdown.

You definitely need to know your employees well, that is to say capabilities, in terms of bringing out the best out of a specific task, to get growth most importantly skill set, expertise is involved and needed in terms of problem solving and creativity to ensure the company grows, no matter one’s awareness, some employees tend to have weak spot, putting out nonchalant behaviour on very important issues.

But been concerned and ensure to create the awareness this way reduces risk, threats and attack coming to the company from the employees.

**WHAT IS THE FIRST SECURITY PRACTICE EMPLOYEES NEED TO BE AWARE OF?.**

The first practice an employee needs to be aware of is that security starts with them and be made aware of the baseline, and most importantly the basic security awareness

Employees are supposed to know the all the cyber security policies in the organisation and to be aware of basic security, which therefore they have to know, what it means to say basic security, this is a process whereby a person understand that there is a potential for some people to deliberately or accidentally steal, damage or misuse the data that they store in an organization system so as to track that particular organisation, knowing this is definitely a first step to take as an employee to know the basic security awareness.

Having been aware of the basic things of security, employees should go further in knowing the first security practices, all employees are supposed to take note and be aware of social engineering, physical security, phishing attack, malware awareness, social media security, Email- security, mobile security and many more, most importantly ensure employee’s bring their own devices, strong passwords and authentication are very necessary.

This awareness is important because 70% of data breaches are happening today nor because of some smart hacker who wants to do your company harm but because of your own employees who has failed in each of these parts due to the fact that they neglect, the basic important things of security that they are are supposed to be Enlighted, and also understanding about circumventing security protocols, disrupting the intended functions of systems of collecting valuable information and not getting caught.