Addressing the Risk Challenge of Internet of Things (IoTs)

By Dr Jimson Olufuye, Chair AfICTA @ IGF2017 Workshop on Internet of Things: Supportive Role of Smart Solutions in the Decision Making Process. 19/12/2017

Introduction

As there are already about 12 billion Internet of Things (IoT) devices connected today, it is projected that by 2020 the figure would rise to more than 35billion. Access to the Internet has made living conditions better over time, and as such, decision makers have continued to rely on IoT devices and smart solutions to enhance decision making process in the area of health management, transportation, communication, security management, home management, office management, sustainable development, governance, accounting. Payments, auditing etc. Critical to IoTs benefit realization is the issue of the associated security risks which if not properly address could cause the loss of private data, assets, money, reputation, business and even life.

The case for Addressing the Risk Challenge of IoT

Many high level distributed denial of service (DDoS) attack witnessed in recent times have prompted strong focus on the security of IoT devices. In the attack on Dyn, over 1million devices were involved for which 96% were IoT devices. The devices were compromised and turned into thingbots. Thingbots are botnets of infected IoT devices that can be used to launch attacks.

The US Food and Drug Administration issued safety advice for cardiac devices over hacking threat, and St. Jude Children's Research Hospital patched vulnerability medical IoT devices. Also, hackers demonstrated a wireless attack on the Tesla Model S automobile. Researchers hacked Vizio Smart TVs to access a home network.

Therefore, there is need to resolve to address IoT device security at various levels - hardware and software, government and enterprise, consumers and services. Indeed, the primary issue is with IoT hardware, which is manufactured without any form of regulation. Regulation is seriously required in this regard. The retail industry has been the leading adopter of IoTs technology because it connects directly to numerous customer base, unlike the health care sector, which does not have benefits that are transparent immediately to the end user and has higher risk.

Again, the need for IoT security cannot be overemphasized when we consider many cases of missed security opportunities occurring during IoT installation and post-installation configuration. You find for example many devices being installed and left unhardened with default user ID and passwords which are well known in the industry. So, IoT security needs to be implemented holistically and it requires understanding of IoT Ecosystem, standards, frameworks and regulatory proposals that have developed recently.

IoTs Ecosystem

The IoT ecosystem is underpinned by information security consideration over cloud computing and analytics process environment. It encapsulate the

hardware manufacture stage (Chip & device) with embedded firmware (software), connectivity (communication), platform and integration (service).

IoT Standard and Framework Development

One of the positive outcomes of the Dyn DDoS attack was the US Department of Homeland Security (DHS) release, in 2016, of principles and guidelines for securing the IoT. These guidelines are not legally mandatory, but are definitely a sign of a good start towards IoTs device security.

Some of these guidelines though known to most security professionals are:

1. Leverage security from the feasibility phase
2. Apply security updates, patching and vulnerability management
3. Follow proven security practices
4. Prioritize controls based on the magnitude or impact
5. Provide oversight and proper governance of the IoT
6. Plug in the device off network if there is no absolute business need.

The Industrial Internet Consortium primarily comprised of IoT - related enterprises, rolled out the Industrial Internet Security Framework (IISF) which outlines best practices to assist developers and end users with gauging IoTs risks and possibly defending against the risks.

Also, the nonprofit Internet of Things Security Foundation (IoTSF) supports all IoT manufacturers, vendors and end users to help secure IoT devices. Notwithstanding, the best countermeasure to combat the hardware vulnerabilities is to regulate the process of manufacturing an IoT device so that manufacturers of IoT devices can be accountable for not adhering to the appropriate IoT regulatory standards, industrial standard and /or guidelines.

Conclusion

Decision makers are increasingly becoming more reliant on IoTs to enhance decision making processes. This is good as optimum decisions are always made when all necessary data and information are available. However, the challenge of risk to IoTs is high at this point at the hardware and software (firmware) levels thereby necessitating calls for regulation and for enterprises to take holistic security measures based on existing IoT devices and the future ones to be deployed.