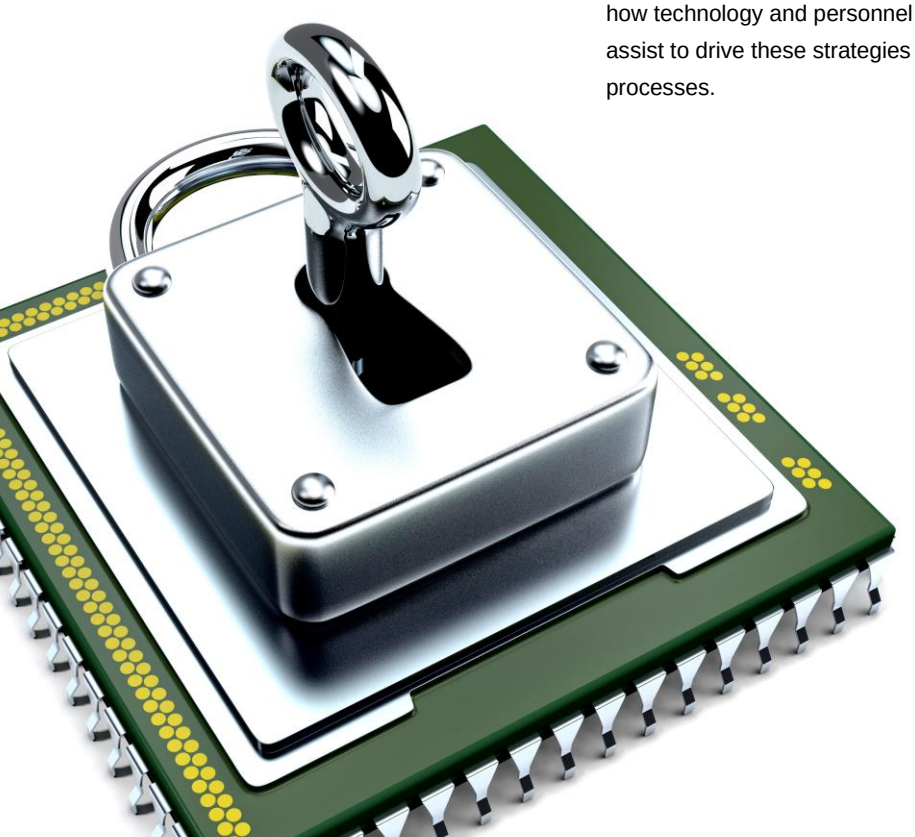
Deloitte.

Why companies may need to implement new security architecture in a cashless society

Tope S. Aladenusi and Omobolaji Vincent

The current security architecture of many Nigerian companies can be likened to a house that has a wooden foundation, glass walls and a steel roof. This is one major reason why despite the recent huge investments in information security by some companies, there are still many “cracks in the wall” and security breaches easily undermine such investments. What do we mean by this?



Let’s take the financial institutions as an example. Over the years, many companies have been very reactive as regards security because their security architecture was driven by the prevalent security issues or regulatory requirements at the time. They probably have never come together as a business to draw up a comprehensive security architecture that aligns with the organisation’s strategic direction, or that defines the organisation’s DNA for security processes, and explains how technology and personnel will assist to drive these strategies and processes.

There was a time when the major issue faced by Nigerian Banks was centred on ATM fraud; major security investments at that time had one singular goal – to reduce ATM fraud. As a result, many banks experienced a significant decrease in ATM fraud over time. Also, there was a time when the Central Bank of Nigeria (CBN) mandated banks to implement the Payment Card Industry Data Security Standard (PCIDSS) and banks had to develop target architecture that met the PCIDSS requirements. This only addressed cardholder data, and there were still untendered and vulnerable areas in some banks’ adequate security investments.

The current practice in several organisations is to continue to build upon existing security architecture designed for specific battles in the past to address new security threats as they arise. This model usually leads to problems, as it is very costly and likely to lead to a lot of wastage.

Once the base is weak, the building faces a high risk of collapse. With the advent of the cashless society, companies can lose a significant part of their shareholders value at the click of a button.

According to a recent review of the cashless system in Nigeria, it was reported that Point of Sale (POS) deployment increased drastically from about 5 000 in 2012 to 153 167 as at April 2014. Transactions valued at ₦24billion were recorded in April 2014, compared to ₦99million in January 2012. If we have these numbers just from POS terminals, then it is only left to the imagination the amount of funds traversing other electronic channels – but more disturbing is the risks posed by threats to these transactional media.

How to develop and implement a security architecture?

In tackling these new security challenges, organisations need to revamp their security architecture to a more robust one that addresses the threats holistically. The most important piece of developing security architecture is aligning the organisation's business needs to its security requirements. The security of any organisation should be a board issue, as it impacts the organisation’s strategic position and brand. Security has to be implemented in a top-down approach, with the board setting the tone, direction and tolerable risk levels. The board should align the security of the organisation to its strategic goals and hand it over to management for implementation.

Management activities should include planning, implementation, execution and monitoring of security initiatives in alignment with the direction set by the board. For example, if an organisation like an online retail store, has the business objective of becoming Nigeria’s biggest online retail shop, the organisation’s security practices have to align with that vision. We will expect to see policies that talk about risk associated with online transactions, and then security measures/controls will be put in place to address identified risks.

A key question that needs to be answered is “What assets are we trying to protect?” You cannot protect what you do not know. Organisations need to have an inventory of all information assets (hardware, software, databases, interfaces among systems, etc.), then classify and segment the assets based on how critical they are. This becomes the basis for deploying security measures to each asset class or segment. For example the “security fence” built around the internet banking server of a bank may be different from the security around a receptionist system. However, many organisations do not have a document showing the number and complexity of systems in place; this in itself is a potential security issue. Some have built a “high wall” around some critical systems; however, these critical systems have a trust relationship with some other systems that are not so critical. Hackers simply exploit the non-critical system and ride on the trust relationship in compromising the critical system, thereby bypassing all the seemingly stringent preventive security measures earlier put in place.

After identification of the assets that are critical to the successful running of the organisation, one needs to identify and classify possible threats that the assets may be exposed to. Having the necessary tools and mechanisms to identify and classify security threats is crucial. This process is called risk assessment, and it forms part of the foundation of an effective security architecture. Other steps required in developing and implementing a proper security architecture, which will not be expanded upon in this article, include steps such as formulation of functional and physical target security architecture designs, development of policies and procedures, and the implementation of the target security architecture designs and integration of security practices to maintain secure status.

There is no such thing as a perfect system. Likewise, no security measure is ever perfect. As security comes at a cost, it may appear that the investment in security is a waste of resources, since perfection cannot be attained. Just because perfect security is not possible does not mean that security cannot be better. Most times security systems fail because they were poorly implemented. Security testing should be in place to ensure that the security systems are working as intended and that they yield adequate returns on investment. There is an adage that says: a nose cannot smell its own odour. What this simply means is that it may not be possible for you to properly and objectively assess your security state. Organisations need to engage external parties to periodically evaluate the capabilities of the organisation in dealing with latest security threats and to perform security assessments to check how vulnerable the organisation is.

The objective of this kind of assessment is simply to find and plug the holes before actual hackers do. So, the assessors wear the hat of an actual hacker and see how far into the organisation's network they can compromise. The assessors then inform the organisation about the issues that led to the compromise for the organisation to fix.

In conclusion, security is not a football match that can be won at the last minute. Organisations need to properly plan their security implementations for full effectiveness. It is time we rethink our security measures by developing and implementing a robust security architecture that is best suited to tackle current security challenges, especially as we continue to embrace a cashless society.

Tope Aladenusi and Omobolaji Vincent work as cyber security specialists at Akintola Williams Deloitte.

For more information contact us on +234 (1) 271 7800 or via email at taladenusi@deloitte.com