Resilience for banks and other businesses in a cyber-attack Incident.

Dr Norman Mugarura

The Banking sector and financial market infrastructure needs to continually train to understand the nature of cyber-attacks and be able to mitigate their adverse effect on the sector. Similarly, individual firms will need to devise individual cyber-attack response mechanisms early enough before they have been attacked. In this regard, it is imperative for firms to enhance efforts aimed at cross sector communications and coordination and information sharing. This could be coordinated either by Bank of Uganda (BOU) or other oversight agencies to ensure a well-co-ordinated robust response in the event of a cyber-attack. There is an adage that "if you wish for peace you will have to prepare for war" and thus, firms cannot complacently wait to be attacked, but to train robustly in advance of cyber-attacks. Let firms carry out simulation exercises during in-house training to validate and rehearse their existing response measures and test their resilience in a real cyber-attack incident. It is important to continually identify areas for improvement, co-ordinated through a single coordination regulator, either BOU or any of its ancillary agencies. A single coordination body is essential to manage communications and information sharing during a real cyber-attack incident. Financial institutions should regularly review their internal cyber-incident response mechanisms and harness experiences of countries such as the USA (which have experienced more incidents of cyber-attacks) and how they have responded to those attacks. I see nothing wrong for regulators to adopt successful regulatory models in other jurisdictions to meet regulatory challenges at home. However, models adopted from foreign jurisdictions will need to be tailored to the domestic regulatory environment to work better.

It is no brainer, the modern communication technology has created vast development opportunities but where goods things abound, criminals are always larking—watch out! The email has become the predominant mode of communication in offices and externally. Emails are used to communicate daily often without a second thought of inherent risks, but note that criminals have exploited them to hack into the data systems of businesses and governments to further their criminal underworld. The email communication has become an instrument for criminal exploitation to create a phoney email account in your name, to set up phoney emails and phone numbers in the name of a real business/firm and used to defraud money from a financial institution or a bank. The US authorities have traced the emails and phone number

used to defraud money from US Banks in Germany, France, Israel and Russia. This signifies that the threat of cybercrime attack is real, live and kicking, government and businesses cannot afford to sit back to be attacked before they devise adequate responses. It is no longer business as usual.

While cyber-attacks are commonly committed in developed countries such as the USA and UK, because of high usage of internet communication technology, in a globalised world, countries are all in it together. I opined in my previous articles in this paper the need for governments and businesses to enhance their budgets to meet the bourgeoning costs of ongoing training and compliance requirements by firms.

For enhanced understanding of cyber-attacks and how to respond during a cyber-incident, banks and other financial institutions need to continually review their processes used to instruct payments through correspondent banks. Criminals have been known to launch attacks on the financial system through correspondent or agent baking. Correspondent banking has particularly been exploited by criminals in countries like Mexico to circumvent tight anti-money laundering/countering financing of terrorism regimes in developed countries to transmit proceeds of crimes into Banks in London and New York. Governments and businesses it is no longer business as usual, you have limited options but to be proactive!

The author is a financial law expert and University lecturer