Creating awareness and improving the prevention of cybercrime

The AfricaHackon convention in Nairobi was an opportune time to discuss a common agenda on information security, largely an unknown subject among many Kenyans. Trends in the marketplace like the increasing speed-to-market of applications and the sophistication and collaboration of hackers indicate a worrisome state of affairs. Conferences of like-minded and ethical security experts like AfricaHackon help to combat these threats through collective and innovative thinking.

The frequency of information security cybercrimes is increasing in Kenya. In the past, Kenya was not a target for cybercriminals but global connectivity means that Kenya is now part of the global cyber environment and therefore as much at risk as anywhere else. Detection technologies can help to reveal more crimes but the frequency and value of crimes is still rising.

It is our view that people themselves are the best defence against information security attacks. Corporates and governments tend to invest in protection technologies but in our view, the solution is not to buy more sophisticated tools. First, it is necessary to understand the concepts behind information security. You can have a very good firewall, for example, but understanding the concepts and principles behind information security is still the best defence.

Unfortunately, it is a lack of understanding by the end-user about the kind of information that hackers actually want that leads to financial crime, reputational damage and intellectual property theft. Users who are not aware of what could happen or when an attack is coming can be the weakest link that undermines all of the investments that an organisation has made in technology.

This lack of understanding occurs at all levels of organisations, including the Board level. When decision-makers do not understand the risks of cybercrime and nature of information security, areas like security budgets suffer.

Strategies to strengthen information security

One strategy that works is to go to a Board with an example and a demonstration of how hackers were able to infiltrate a system and then show Board members what is possible in terms of solutions. Although there is no one-size-fits-all solution for any organisation, the demonstration can help to open their eyes to the danger of cybercrime and the solutions that can be tailored to the organisation's needs.

So-called 'ethical hackers' seek permission and define the boundaries of a penetration test which can also indicate the potential financial impact. Very often, we encounter surprise when the demonstration shows the financial impact of a hacking. Quite quickly, decision-makers realise that they need budgets; technology tools, people and processes to prevent and detect cyber security breaches.

Going forward, we can expect hackers to get smarter simply because technology is moving very fast—faster than the people who are developing solutions and their shared knowledge within the community of information security experts. There is more collaboration within the hacker community as compared to the defensive security community. Collaboration creates an environment of innovation which is a critical success factor for both defensive security solutions and nefarious hacking.

Inter-territory collaboration for reporting and sharing information between countries and governments can help to protect citizens and organisations. Government agencies like

Kenya’s CID and the US’s FBI do work together but there are still gaps. Government officials and people developing relevant legislation need to understand what exactly they should legislate so as to align government policy with actual risks in the marketplace and to ensure that enforcement is empowered by capacity and expertise.

Globally, financial institutions and telecommunications companies tend to be amongst the top targets for information security criminals because they have sensitive and valuable information. Many of these organisations focus on technology solutions instead of policy, processes and people. They may not have an information security expert on their Boards of Directors. They insure themselves against risk and, at the end of the day, they hope for the best. When information security breaches occur, these and other institutions may hesitate to share information about the breach since it poses a reputational risk.

A central repository of information would help to stop perpetrators from jumping from organisation to organisation and if it was housed within a secure, international, governing agency then the information would remain confidential but could also be used to fight crime.

The future looks a bit scary; with so much of our information online, cyber security is becoming a global and national security concern. Fortunately, there is a growing community of cyber security specialists who share information about the latest trends and changes in the security environment. Going forward, it will be important to empower more communities that are driving the information security agenda through convergence and awareness in the marketplace.

George Wahome is a Manager and Munir Njiru is an Assistant Manager with PwC Kenya’s IT Risk Assurance business.