Enhancing Cybersecurity for Critical Business Infrastructure in Africa

As the world continues to recover from the disruptions of the COVID-19 pandemic and the Ukraine – Russia conflict, coping mechanisms such as increased use of virtual workspaces, online marketplaces and e-governance have become the norm. While this presents opportunities to revamp economies and streamline public service delivery, it may also heighten exposure to cybercrime.

According to a special report by Cybercrime Magazine, the global cost of cybercrime is expected to reach an estimated USD 6 trillion by the end of 2022 and USD 10.5 trillion by 2025. These estimates represent a significant leap in the frequency and scope of cybercrime which reached a record high of approximately USD 1 trillion in 2020. Out of the 2020 estimation, approximately USD 945 billion was lost due to cyber-attacks, and approximately USD 145 billion was spent on cyber security efforts. The increase in reported cybercrime has been attributed to various factors, including the increase in online activity which has resulted in increased reporting of incidents by governments and organisations.

Despite this trend, businesses have fallen behind in implementing robust cybersecurity measures. For instance, it is estimated that 20 percent of organisations worldwide do not have any cyber incident prevention plan in place. Similarly, a cybersecurity benchmarking study carried out in 2022 revealed that 41 percent of the polled executives were not confident that their security initiatives aligned with the current digital transformations. These vulnerabilities put organisations and their stakeholders at significant risk. Attacks on critical infrastructure, such as in the power, communications, financial, health and transportation sectors, are of particular concern given the impact that such disruptions can have on large segments of the population and the threat that they pose to national security.

In Africa, many countries have seen a rise in reports of digital threats and malicious cyber activities. The results include sabotaged public infrastructure, losses from digital fraud and illicit financial flows, and national security breaches involving espionage and intelligence theft by militant groups. Addressing these vulnerabilities requires a greater commitment to cybersecurity. This requires enforceable policy safeguards, risk prevention and management approaches, along with technologies and infrastructure that can protect each country’s cyber environment, as well as individual and corporate end-user assets. This, therefore, helps institutions, and public and private entities to mitigate risks associated with cybercrime and to enhance cybersecurity.

Africa’s digital transformation has made information much more valuable and many countries are in the process of ensuring that there are conducive legal and regulatory frameworks, in order to prevent information from being accessed illegally and without consent. In a bid to create these frameworks, governments are also aware that they should not underpin the growth of the digital space. For instance, a 2022 survey done by the Central Bank of Kenya reveals that 92 percent of banks and 86 percent of microfinance banks identified cyber-risks as one of the top three innovation-related risks. In a way, the world of cybersecurity is an evolving one as malicious individuals and organisations are constantly looking for improved ways of accessing data and information. It has been clear that the digital revolution has positively affected some industries more than others such as banking & finance, media & telecommunications and technology. Despite the positives, the risks are also quite significant.

Given the vulnerability of various industries to cybercrime, significant effort must go towards planning for the prevention of cyber-attacks and, where prevention is not possible, mitigating their effects when they do occur. Protecting critical infrastructures, such as power stations, transportation, telecommunications, financial services, and water supply is particularly important given the significant risk that any disruption poses. Below are some of the critical mitigating risk factors that should be put in place.

Awareness

A critical step is to create awareness of how cyber-attacks may be perpetrated. The most frequent form of a cyber-attack on critical infrastructure globally has been through malware, including ransomware, which compromises internal systems disrupting their functionality. Additionally, these attacks cost countries significant losses especially if there is a disruption in power supply as a result. Therefore, governments and private entities must step up measures to educate the public on how these attacks may be carried out.

Training

It is important to train those who interact with the infrastructure on how they may prevent or mitigate cyber-attacks. Crucially, given the interconnectedness and interdependence of the supply chain systems, cybersecurity preparedness should take a collaborative approach. For instance, the banking and finance and telecommunications sectors in Africa have become interdependent and operate in the same ecosystem, especially because of mobile banking which is crucial for most businesses.

Design, Auditing and Monitoring

For new systems being developed, ‘resilience by design’ should be considered, which includes cybersecurity as a parameter in the design of the infrastructure. This will reduce the chances of an attack taking place. To ensure that the critical infrastructure is secure enough, an audit ought to be undertaken to identify any faults or improvements that may need to be made. Furthermore, several tools exist which constantly monitor relevant threats by identifying indicators of compromise affecting technological systems on a real-time basis.

Risk Management Plan

A plan in the form of a risk management manual should be laid down. This plan should require the infrastructure and related systems to be evaluated frequently. In the event of a cyber-attack, it is important to have a team that is well versed in crisis management in the context of cybersecurity. This requires having the people with the right skills to quickly enable the affected organisation to identify the root causes of the cyber-attack, address the problem and move on from the situation better prepared to mitigate such risks in the future.

As Africa continues to grow in leaps and bounds within the digital space, vigilance should be a guiding principle. Governments should ensure that they are able to invest in cybersecurity and monitor malicious activity without invading the privacy of their citizens. To ensure that they can achieve all this comprehensively, they must involve the public in the decisions they make as well as come up with legislative changes that can be enforced in incidents of cyber-attacks.

Business Daily | Cybersecurity Ventures | ITU | The East African