ALN
KENYA
Anjarwalla & Khanna

Combating Cybercrime on Critical Infrastructure in the Region

JULY 2022

Introduction

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.[1] These estimates represent a staggering 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.[2] The increase in reported cybercrime has been attributed to various factors, including the increase in online activity brought about by the COVID-19 pandemic as well as better awareness of cyber-attacks, 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 one-fifth (20%) of organisations worldwide do not have any cyber incident prevention plan in place.[3] Similarly, a cybersecurity benchmarking study carried out in 2022 revealed that 41% of the polled executives were not confident that their security initiatives aligned with the current digital transformations.[4] 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. For example, the US Department of Energy considers cybersecurity in the energy sector as one of the nation's key national security challenges.

Cyber-Attacks on Critical Infrastructure

Over the years, critical public and private infrastructure has been the target of global cyber-attacks in various forms, including malware, phishing, password, man-in-the-middle, Structured Query Language injection, and Denial of Service (DOS) attacks, as well as insider threats, crypto jacking, and zero-day exploits, to name a few.

The digitisation and increased networking of critical infrastructure at the levels of production, storage, transport, and consumption render this sector particularly vulnerable.[5] One of the earliest reported cyber-attacks on critical infrastructure was in 2003 when the safety parameters display system of the Davis-Besse nuclear plant in Ohio stopped for a couple of hours due to infection by the Slammer computer worm, impacting the system that would trigger an alarm in the event of a reactor meltdown. Its compromise, although without any devastating effects, was of great concern.

East Africa has also reported cyber-attacks that targeted critical infrastructure, with a focus on the financial sector. For example, in 2017, Kenya's largest telecom operator, Safaricom, managed to thwart an attempted attack by hackers seeking to gain access to customer funds on its mobile money transfer platform M-Pesa.[6] In 2018, the National Bank of Kenya, now a subsidiary of KCB Group, admitted to losing approximately KES 29 million in a fraud attack on the bank. In July 2021, eight Kenyan nationals and a Ugandan national were jailed in Rwanda for hacking the system of a key regional bank to access client accounts and funnel the funds to Rwandans. The individuals are also suspected to have successfully conducted similar hacks in both Kenya and Uganda.[7]

Cybersecurity concerns in the banking sector remain, as demonstrated by a 2022 survey by the Central Bank of Kenya which revealed that 92% of banks and 86% of microfinance banks identified cyber-risks as one of the top three innovation-related risks.[8]

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

More recently, on 4 May 2022, the Director-General of the Ethiopian Information Network Security Agency (INSA) reported that INSA had intercepted an international cyber-attack attempt on the Grand Ethiopian Renaissance Dam that targeted 37,000 interlinked computers used by financial institutions and the country's major financial institutions.[9]

The Director-General alleged that the attack was perpetrated by a malevolent state but did not disclose the name of the sponsoring country. This attack comes on the back of a rapid increase in cybercrime in Ethiopia which has witnessed a record high of more than 5,000 reported cyber-attack attempts during the 2021/2022 fiscal year. The figure has quadrupled compared to attacks recorded during the same period in the last fiscal year. The targeted institutions include Government ministries, academic institutions, regional bureaus, and media houses.[10]

The number and technical complexity of cyber-attacks on critical infrastructure has increased over the years, as well as awareness of the threats.[11]

The digitisation and increased networking of critical infrastructure at the levels of production, storage, transport, and consumption render the infrastructure sector particularly vulnerable

Kenya: Cyber-Attacks and Its Regulatory Landscape

According to the Communications Authority of Kenya's statistics for the period of July-September 2021, the National Computer Incident Response Team (CIRT) detected more than 143 million cyber-attacks in Kenya. This is an increase from the approximate total of 38 million threats detected in the previous period between April-June of the same year. Most of these cyber-attacks were malware attacks which accounted for 70 million of the total figures. Small businesses were particularly vulnerable as they witnessed a 47% increase in internet attacks. The increase is attributed to the rise of remote working systems as well as increased e-commerce activity spurred by COVID-19.[12]

In the context of cybercrime regulation, at the international level, the Convention on Cybercrime, 2001, which came into force on 1 July 2004, is the first international treaty on crimes committed via the Internet and other computer networks. It deals particularly with infringements of copyright, computer-related fraud, and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

The Convention's main objective is to pursue a common criminal policy which is aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.[13] However, Kenya is not currently a signatory to the Convention.

According to the Communications Authority of Kenya's statistics (July-September 2021), the National Computer Incident Response Team has detected more than 143 million cyber-attacks in Kenya

In Kenya, the primary legislation that provides for cybercrimes is the Computer Misuse and Cybercrimes Act, 2018 (the Act), which provides for offences relating to computer systems with the aim of enabling timely and effective detection, prohibition, prevention, response, investigation, and prosecution of cybercrimes. The Act is also intended to facilitate international co-operation in dealing with computer and cybercrime matters.[14] Further, the Act establishes the National Computer and Cybercrimes Co-ordination Committee (the NCCCC) whose mandate includes advising the Government of Kenya on cybersecurity.[15]

Other legislation that specifically addresses cybercrime includes the Kenya Information and Communication Act, 1998, the Penal Code, 1930, the Evidence Act, 1963, the Data Protection Act, 2019, and the Central Bank of Kenya Guidance Note on Cybersecurity. Additionally, the various Government bodies that play a role in combating cybercrime include the Ministry of Information, Communication and Technology, the Cyber Crime Unit of the Directorate of Criminal Investigations (DCI-CC), the Communications Authority and the NCCCC.

A 2022 survey by the Central Bank of Kenya reveals that 92% of banks and 86% of microfinance banks identified cyber-risks as one of the top three innovation-related risks

Mitigating Risk

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 infrastructure, such as power stations, transportation, telecommunications, financial services, and water supply is particularly important given the significant risk that any disruption poses.

Awareness: A critical step is to create awareness on 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 compromise internal systems disrupting their functionality.

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.[16]

Design, Auditing and Monitoring: For new systems being developed, 'resilience by design' should be considered, which involves including 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 to 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 root causes of the cyber-attack, address them and move on from the situation in better shape.

ALN
KENYA
Anjarwalla & Khanna

Key Contacts

Should you have any questions on cybercrime, cybersecurity, and data privacy in the context of Kenya, please do not hesitate to contact:

Luisa Cetina
Director
ALN Kenya | Anjarwalla & Khanna

Anne Kiunuhe
Partner
ALN Kenya | Anjarwalla & Khanna

Willie Oelofse
Director
ALN Kenya | Anjarwalla & Khanna

Contributors
Ian Kanja Njogu, *Associate*
Jade Makory, *Associate*
Kelly Nyaga, *Trainee*
Chebet Korir, *Intern*

Endnotes

1 Steve Morgan, ‘Cybercrime To Cost The World $10.5 Trillion Annually By 2025’ November 2020.

2 Zhanna Malekos Smith and Eugenia Lostri, McAfee, ‘The Hidden Costs of Cybercrime’, December 2020.

3 CIO Axis, ‘Cybercrime cost the world more than $1 trillion in 2020’.

4 ThoughtLab, ‘Cybersecurity Solutions for a Riskier World’.

5 Gabrielle Desarnaud, Etudes de l’Ifri, ‘Cyberattacks and energy infrastructures’.

6 Citizen, Ephraim Mugo, ‘Safaricom thwarts cyber attack attempts’.

7 The East African, Otiato Guguyu, ‘Rwanda jails 8 Kenyans, Ugandan in Equity Bank hacking case’.

8 The Kenyan Wall Street, ‘Cyber Attacks Remain Key Risk in Online Banking – CBK’.

9 The East African, ‘Ethiopia ‘Foils’ cyber-attack on Nile dam, Financial Institutions’, 4 May 2022

10 The East African, ‘Cyber-attacks more than quadruple in Ethiopia: intelligence agency’, 11 May 2022

11 Gabrielle Desarnaud, Etudes de l’Ifri, ‘Cyberattacks and energy infrastructures’.

12 Business Daily, ‘Cyber-attacks in Kenya up by half to hit 56m in three months’.

13 Council of Europe, ‘Details of Treaty No.185, Convention on Cybercrime’.

14 Long Title, Computer Misuse and Cybercrimes Act, 2018.

15 Section 6 of the Computer Misuse and Cybercrimes Act, 2018.

16 World Economic Forum, ‘The US pipeline attack shows the energy sector must act now on cybersecurity. Here are 6 ways how’.

*The content of this article is intended to be of general use only and should not be relied upon without seeking specific legal advice on any matter.

ALN Kenya | Anjarwalla & Khanna is a member of ALN, an integrated alliance of preeminent full-service corporate law firms in 15 African countries and a regional office in UAE.

ALGERIA | CÔTE D’IVOIRE | ETHIOPIA | GUINEA | **KENYA** | MADAGASCAR | MALAWI | MAURITIUS |MOROCCO | NIGERIA | RWANDA
SUDAN | TANZANIA | UGANDA | ZAMBIA • UAE