Executive Summary:
2018 Africa Cyber Threat Intelligence Report (ACTIR)

A new study from Cyber Security firm **Jighi** sanctioned by the 2018 Africa Cyber Security Conference (ACSC) shows the pervasive nature of cybercrime across the continent, affecting businesses, individuals, families, financial institutions, and government agencies. The study, which was mainly performed by Jighi's advanced cyber security unit, **Enovise**, claim that weak security architectures, scarcity of skilled personnel, lack of awareness and uncoordinated regulations in African countries have increased the continent cyber vulnerability.

Sophisticated malware, software security breaches, mobile scams—the list of cybercrime threats is growing. Yet African nations continue to fall short of protecting themselves and must constantly grapple with the impact. And it is a heavy impact: cybercrime costs the continent an estimated $3.7 billion in 2017.

Among the many findings, the report also shows that more than 90% of African businesses were operating below the cybersecurity "poverty line"—meaning they couldn't adequately protect themselves against losses. At least 96% of online-related security incidents went unreported and more than 70% of organizations didn't keep up to date with cybersecurity trends and program updates.

To make matters worst, many official agencies didn't know the extent of the digital risk they faced even as governments, including Cote D'Ivoire, Benin, Kenya and Tanzania, have been automating services and moving to digital services (transformation numerique)—making them prime targets for hackers. Dozens of sites belonging to the Kenyan and Nigerian governments have been hacked in the last 18months, highlighting their vulnerability. Banks, Payment Service Providers (PSP) and internal-revenue authorities in Africa are getting hit the most, with hackers getting away with millions.

Amongst other findings, the study highlights that threats and risks are above and beyond financial losses only. It demonstrates the increased presence of diplomatic hacking or state sponsored hacking as some may call it. Although the report singles out China as the main threat actor in this area, it clearly shows other Western nations engaging in the same spying/hacking activities. These so called "friendly hacking" show how other countries are clearly taking advantages of their African friends. The report calls for African countries to better protect their digital assets (political, diplomatic, industrial, energie, telecom and financial).

However, the reports cautioned that dealing with cybercrime will continue to be problematic because even though the cyber security market will be worth $2 billion by 2020, Africa has yet to produce a single commercially viable cybersecurity product or solution. Obviously, this begs for more training and education in computer science and the science of IT security.

In addition to a slew of recommandations to the political and business leadership, the report stresses that businesses and banks in particular should upgrade outdated systems, put competent IT personnel in charge of configuring/maintaining systems, hire renown security /IT technology companies, and perform regular infosec audit/pentests. It strongly suggest that cyber security be part of every online service and that more employees and individuals be trained to be aware of the risks that evolving cyber threats like phishing poses to the organisation. Finally, the report calls on African governments to hire reputable cyber security firms to monitor and gauge the threat potential of contracting firms and vendors who work on critical infrastructure.

A full copy of the report can be obtained from acsc@jighi.com 10/25/2018