Kenya Bureau of Standards

Standards for Quality life

NL:00.kl.10 2024

NEWSLETTER

KEBS CELEBRATES 50TH ANNIVERSARY DURING WORLD STANDARDS DAY ON 14TH OCTOBER, 2024

Head of the Public Service, Felix Koskei (2nd left) is joined by the Cabinet Secretary in the Ministry of Investment, Trade and Industry, Salim Mvurya (extreme left), Kenya Bureau of Standards Managing Director, Esther Ngari (centre), Principal Secretary in charge of Industry at the Ministry of Investment, Trade and Industry, Dr. Juma Mukhwana (2nd right) and Chairman of the National Standards Council, Anthony M. Munyiri (extreme right), in pressing a buzzer to commemorate this year's World Standards Day, and KEBS' 50 anniversary at KEBS Headquarters.

IN THIS ISSUE

KEBS Celebrates 50 Years of Setting Quality Standards

KEBS was launched in 1974 and is now an important component in Kenya's Development journey

KEBS' CELEBRATES 50 YEARS OF CONSUMER PROTECTION AND QUALITY ASSURANCE

By Solomon Kyenze

The Cabinet Secretary, Ministry of Trade, Investment and Industry, Salim Mvurya, while addressing celebrations to mark the World Standards Day during which the Kenya Bureau of Standards commemorated its 50th Anniversary. The event was held at the KEBS Headquarters.

Kenya Bureau of Standards (KEBS) celebrated its 50th anniversary on October 14th, 2024, with stakeholders in the standards sector seizing the moment to reflect on a half a century legacy of developing Kenya's standards.

Senior government representatives including the Head of the Public Service, Felix Koskei and the Cabinet Secretary in the Ministry of Investment, Trade and Industry, Salim Mvurya joined the KEBS fraternity and other key players in the sector to commemorate the Golden Jubilee at the KEBS Headquarters.

The event, which was marked with pomp, moving speeches, and a recognition of various players instrumental in the KEBS history, also coincided with celebrations to mark this year's World Standards Day which is commemorated annually on the 14th October, 2024.

Established in 1974 under the Standards Act, Cap 496 of the Laws of Kenya, KEBS has continued to play an important role in ensuring the quality, safety, and competitiveness of products and services, both locally and internationally.

Its mandate is to protect Kenyan consumers by developing, promoting, and enforcing standards that ensure goods and services are reliable and safe. Through its regulatory framework, KEBS has fostered industrial growth, improved product quality, and enhanced the nation's economic transformation.

Additionally, it has played a critical role in elevating Kenya's position in global trade by ensuring that Kenyan products meet international standards, KEBS has helped local businesses gain a competitive edge in global markets, driving economic growth, and contributing to the nation's development. From agricultural products to manufactured goods, standards have ensured that Kenya can compete favorably on the international stage, building trust in the "Made in Kenya" label.

Speaking during the celebrations, the Head of the Public Service who was the chief guest noted that quality standards play a pivotal role in promoting good governance and enhancing service delivery in Kenya's public sector.

"By establishing clear benchmarks for performance, efficiency, and accountability, standards ensure government services are delivered consistently, transparently, and with integrity, helping streamline operations, reduce inefficiencies, and foster a culture of continuous improvement across public institutions", Koskei observed..

He said trust was crucial for the effective running of public service and for efficient governance saying, "At the heart of the public service and governance lies one word- Trust. Good governance is not measured by the mere provision of services, but by the quality, reliability, and integrity of those services. Standards are the custodians of this trust."

Cabinet Secretary Mvurya who was accompanied by the Principal Secretary in charge of Industry at the Ministry, Dr. Juma Mukhwana, described standards as products of rules and regulations, and said every product, service or process in the country must reflect a level of quality and safety that protects the people and propels the country forward in the global market.

Mvurya affirmed the government's commitment to economic transformation through the Bottom-Up Economic Transformative Agenda (BETA) through investment in the development of the manufacturing sector."Manufacturing is at the heart of the BETA agenda. Through initiatives like the County Aggregation and Industrial Parks (CAIPs), we are building hubs where innovation and value addition will flourish. These parks will create jobs, stimulate growth, and position Kenya as a global industrial leader. But none of these will be possible without ensuring that standards are met at every step," Mvurya remarked.

Dr. Mukhwana also hailed the importance of BETA, saying the program was helping shift the center of economic focus to the people at the grassroots ensuring every Kenyan has a stake in the country's prosperity.

In her address, KEBS Managing Director, Esther Ngari, lauded stakeholders in the standards' sector for their critical role in developing and advancing the adherence and conformity to standards to safeguard the safety of consumers and facilitate trade.

"Manufacturers, importers, exporters, and MSMEs are the lifeblood of our standards movement. Whether creating products for local households or exporting goods across the globe, they have elevated 'Made in Kenya' to become synonymous with trust and excellence. Together, we've crafted an ecosystem where standards are not just regulations but a promise to every consumer", she noted.

The Managing Director hailed the impact of the stakeholders, including industry leaders, policymakers, academic institutions, consumers, civil society and media, for their role in ensuring that Kenya's standards remain forward- looking, relevant, and adaptable to the changing global landscape.

She said, "As we mark this 50th anniversary, KEBS is committed to strengthening partnerships and fostering dialogue with stakeholders to entrench sustainability in the standards development process. This collaboration will ensure that future standards not only meet the needs of today but also address the challenges of tomorrow, particularly in the areas of climate action, resource conservation, and social equity".

Ngari expressed optimism for the future stating KEBS' dedication to ensuring standards are the cornerstone of the country's economic growth, and a foundation for building a more resilient, sustainable, and inclusive society. KEBS will also lead in the adoption of emerging global realities that include climate change and redouble its efforts in standards development.

National Standards Council Chairman, Anthony M. Munyiri emphasized the importance of standards, saying they will be instrumental in determining the future of how the world responds to future challenges.

"The future will be defined by how we respond to global challenges. Resilient infrastructures, especially smart cities and communities and the ever-shifting consumer expectations are reshaping industries faster than ever before. In this dynamic landscape, standards will be crucial. They will serve as the blueprint for adapting to change, ensuring that innovation and sustainability walk hand in hand," Munyiri said.

Head of the Public Service, Felix Koskei (centre), while on a tour of the Kenya Bureau of Standards laboratories during celebrations to mark the World Standards Day. He was taken round the facilities by KEBS Managing Director, Esther Ngari (2nd right), and the Chairman of the National Standards Council, Anthony M. Munyiri (right).

WORLD MARKS WORLD STANDARDS DAY WITH FOCUS ON ARTIFICIAL INTELLIGENCE

By Geoffrey Nyerere

Head of the Public Service, Felix Koskei (3rd right), and the Cabinet Secretary, Ministry of Trade, Investment and Industry, Salim Mvurya (centre), cutting a cake to commemorate KEBS' 50th Anniversary during celebrations to mark the World Standards Day at the KEBS Headquarters.

The annual World Standards Day is observed each year on the 14th October.

The local standards sector led by the Kenya Bureau of Standards (KEBS) joined the world in commemorating the day during an event held at the KEBS' Headquarters and that was graced by the presence of among others the Head of the Public Service, Felix Koskei and the Cabinet Secretary in the Ministry of Trade, Investment and Industry, Salim Mvurya.

This year's theme, "Shared Vision for a Better World: Spotlight on SDG 9, Industry, Innovation, and Infrastructure in the Age of AI," puts the spotlight on Sustainable Development Goal 9 (SDG 9), which focuses on building resilient infrastructure, promoting inclusive and sustainable industrialization, and fostering innovation.

The theme resonated well with KEBS' vision of embracing emerging technologies to drive industrialization and infrastructure development in Kenya. KEBS has recognized the importance of AI in shaping Kenya's future and has actively participated in developing standards that govern the safe and ethical use of AI technologies.

These standards ensure that AI is used to foster inclusive growth, promote sustainability, and protect consumers from potential risks associated with technological advancements.

AI has become an integral part of modern industrial processes, offering unprecedented opportunities for innovation, efficiency, and productivity. However, with these opportunities come challenges related to regulation, security, and ethical concerns, all of which require robust standards.

AI-driven innovation has the potential to revolutionize Kenya's industries by automating processes, enhancing service delivery, and improving decision-making. KEBS' role in setting standards for AI applications will ensure that these technologies are implemented responsibly and contribute to the nation's overall economic growth.

KEBS, since its inception in 1974 under the Standards Act, Cap 496 of the Laws of Kenya, has been instrumental in shaping Kenya's development. Over the past five decades, the Bureau has played a pivotal role in ensuring the quality, safety, and competitiveness of products and services, both locally and internationally. Its mandate is to protect Kenyan consumers by developing, promoting, and enforcing standards that ensure goods and services are reliable and safe. Through its regulatory framework, KEBS has fostered industrial growth, improved product quality, and enhanced the nation's economic transformation.

The annual World Standards Day celebrates the collaborative efforts of thousands of experts worldwide who develop the voluntary technical agreements that are published as International Standards.

International Standards are the backbone of global progress. They ensure interoperability, security, and sustainability, fostering global collaboration to accelerate innovation through AI.

This year's celebration held special significance for KEBS as it also marks the organization's 50th anniversary, a milestone in Kenya's journey towards quality assurance, consumer safety, and international trade competitiveness.

World Standards Day, observed every October 14, acknowledges the essential role of standards in improving the quality of life globally. International standards ensure that products, systems, and services are safe, reliable, and of good quality, providing a foundation for global collaboration, trade, and innovation.

Head of the Public Service, Felix Koskei, while addressing celebrations to mark the World Standards Day and to commemorate Kenya Bureau of Standards' 50th anniversary at KEBS Headquarters.

The annual World Standards Day celebrates the collaborative efiorts of thousands of experts

Kenya Bureau of Standards Head of Dosimetry, Grace Ateka, introducing the Head of the Public Service, Felix Koskei (3rd right), and the Principal Secretary for Industry at the Ministry of Investment, Trade and Industry, Dr. Juma Mukhwana (4th right), to the operations of the laboratory when they toured KEBS' facilities during the World Standards Day.

CYBERSECURITY, WHY WE NEED TO BE VIGILANT

By Esther Ngari, Managing Director, Kenya Bureau of Standards

Kenya Bureau of Standards Managing Director, Esther Ngari

Computers and information technology are essential to the mission of any modern organization and KEBS is not exceptional. As a standards agency, we are committed to provide Standardization, Metrology, and Conformity Assessment Services that safeguard consumers and facilitate trade for a sustainable future. In today's digital age, we ought to recognize that cybersecurity is an integral part of this mission.

Today we face increasing threats from malicious cyber-attacks, loss of privacy from spyware and adware, and identity theft and fraud. It is essential that we take a thorough and collaborative approach to managing our cyber security risks to stay ahead of the curve.

Cybersecurity Awareness Month is an international initiative that highlights actions everyone can take to stay safe online. This year mark the 21st Annual Cybersecurity Awareness Month which was founded in 2004 and held each October as the world's foremost initiative aimed at promoting cybersecurity awareness and best practices Kenya Bureau of Standards is Committed to Securing Our World by taking an action during Cybersecurity Awareness Month to Reduce Cyber Risk to our business operations.

We take time this month to highlight the growing importance of cybersecurity in our daily lives and encourage ourselves to take important cybersecurity steps every day to Secure Our World and stay safe online.

KEBS is certified to Information Security Management System (ISMS) based on ISO/IEC 27001:2022 integrated with Business Continuity (BCMS) based on ISO 22301 as a commitment to ensuring that the organization and its employees remain proactive, stay informed about the latest cyberthreats and evolving their strategies to mitigate such risks.

The theme of Cybersecurity Awareness Month is Secure Our World, which encourages all of us to take four easy steps each day to ensure our online safety:

- Appreciating the use of strong passwords and password manager
- Using multifactor authentication on personal devices and business networks.
- Recognize and report phishing
- Install updates on a regular basis and turn on automated updates on our computers.

Let's work together to protect our systems, data, and the trust of the Kenyan public. By promoting a culture of cybersecurity awareness, we can ensure that we achieve our vision of being a global leader in standards-based solutions for trade and sustainable development.

Kenya Bureau of Standards
Standards for Quality life

SECURE OUR WORLD

FIREWALLS

DON'T PROVIDE COMPLETE COVERAGE.

- ✓ Beware of email attachments and links
- ✓ Check privacy settings
- ✓ Don't post personal information

#CYBERSECURITY AWARENESS MONTH

SPECIAL FOCUS ON CYBER SECURITY AS WORLD MARKS CYBER SECURITY AWARENESS MONTH

Kenya Bureau of Standards is Committed to Securing Our World by taking an action during Cybersecurity Awareness Month to Reduce Cyber Risk to our business operations.

Every year October is Cybersecurity Awareness Month, which we take time to highlight the growing importance of cybersecurity in our daily lives and encourages ourselves to take important cybersecurity steps every day to Secure Our World and stay safe online.

October 1, 2024, marks the start of cybersecurity education by participating in the 21st Annual Cybersecurity Awareness Month which was founded in 2004 and held each October as the world's foremost initiative aimed at promoting cybersecurity awareness and best practices.

Cybersecurity Awareness Month is a collaborative effort among businesses, government agencies, colleges and universities, associations, nonprofit organizations, tribal communities, and individuals committed to educating others about online safety.

From mobile to connected home devices, technology is deeply intertwined in our lives. Emerging technologies have many great benefits for society but with those new technologies come new opportunities for bad actors to disrupt our online activities at home, school or at work. Cybersecurity Awareness Month aims to highlight some of the emerging challenges that exist in the world of cybersecurity today and provide straightforward, actionable guidance that anyone can follow to create a safe and secure digital world for themselves and their loved ones.

KEBS is certified to Information Security Management System (ISMS) based on ISO/IEC 27001:2022 as a commitment to ensuring that the organization and its employees remain proactive, stay informed about the latest cyberthreats and evolving their strategies to mitigate such risks.

KEBS
Kenya Bureau of Standards
Standards for Quality life
SECURE OUR WORLD
MULTI-FACTOR, TWO-FACTOR, TWO-STEP...
YOUR CODE
64370
ENTER CODE
6 4
Username@mail.com
****
***
#CYBERSECURITYAWARENESSMONTH

The theme of Cybersecurity Awareness Month is Secure Our World, which encourages all of us to take four easy steps each day to ensure our online safety:

- Understand the benefits of using a password manager and dispelling existing myths around password manager security and ease of use.
- Turn on multifactor authentication on personal devices and business networks.
- Recognize and report phishing – still one of the primary threat actions used by cybercriminals today.
- Install updates on a regular basis and turn on automated updates.

Cybersecurity Awareness Month continues to build momentum and impact with the goal of providing everyone with the information they need to stay safe and more secure online. KEBS is proud to support this critically important online safety awareness and education initiative, led by our Information Security team.

ADDRESSING PRIVACY, SECURITY AND RISK ASPECTS OF DATA IN KEBS

By: Justin Bosire | Principal IT Officer – Network & Infrastructure Management

In the digital age, data has emerged as the new currency, an invaluable asset that powers economies and shapes societies. For Kenya Bureau of Standards (KEBS), the responsibility of safeguarding this treasure is paramount. Yet, the path to effective data protection is riddled with challenges. To effectively protect sensitive information from malicious actors, governments must navigate a complex landscape where privacy, security and risk blend.

Privacy is the foundation of data protection, ensuring individuals or organizations retain control over their personal or proprietary information and are protected from unauthorized access and surveillance. Security serves as the impenetrable defense, shielding data against threats to its confidentiality, integrity and availability (CIA). Meanwhile, risk management acts as the vigilant guard, proactively identifying and mitigating potential threats to data CIA.

The Challenges of Cybersecurity

Protecting data from threats to its CIA has become a critical mission for governments and businesses across the world. But imagine for a moment: What if the very institutions tasked with safeguarding our personal information became vulnerable? This isn't just a hypothetical scenario—it's a challenge that government agencies as well as businesses face every day.

Picture a fortress-built centuries ago, now tasked with defending against modern warfare. That's essentially what many government agencies including KEBS are dealing with when it comes to their Information Security infrastructure. Legacy systems, often decades old and running on outdated software, are the Achilles' heel of government cybersecurity. These systems were not designed to handle the volume and complexity of today's cyber threats, making them prime targets for hackers.

But it's not just about old and outdated technology. The need for multiagency data sharing creates a complex web of vulnerabilities. Every connection point is a potential entry for cyber threats. The more agencies share data, the greater the risk of a breach. This is especially true when data is shared across different levels of government, such as between national and county governments and agencies.

Enhancing Digital Trust

In an age of increasing privacy concerns, citizen trust in the digital ecosystem is both a precious commodity and a significant challenge. When data breaches make headlines, that trust erodes fast. KEBS must work tirelessly to demonstrate commitment to data security and transparency. This includes being open about their data collection practices, responding quickly and effectively to breaches, and holding those responsible accountable.

Battling Budget Constraints

While cyber threats evolve at lightning speed, budgets meant to address cybersecurity threats often move at a glacial pace. Budget constraints force agencies to make tough choices between upgrading systems and other critical services. This can lead to a situation where agencies are constantly playing catch-up, trying to patch vulnerabilities and respond to breaches instead of proactively preventing them.

Imagine waking up to find that millions of citizens' personal data has been exposed. This nightmare scenario is what keeps IT professionals up at night. A data breach can have devastating consequences, including identity theft, financial fraud, and even national security risks. Government agencies like KEBS must have robust incident response plans alongside sufficient resources in place to mitigate the damage and restore public trust.

Risk Management Strategies

Given the complexity and evolving threat landscape within the cyberspace, government agencies are called upon to implement several risk management strategies as discussed below:

- **Regular security audits:** Regular audits can help identify vulnerabilities in systems and processes before they can be exploited. Audits are part of the broader approach to security assessment along with vulnerability assessment and penetration testing.

- **Employee security awareness, education and training programs:** Employees are often the weakest link in cybersecurity. Security awareness and training programs can help modify their behavior as well as educate them about the risks and how to avoid them.
- **Threat intelligence capabilities:** Information relating to information security threats should be collected and analyzed to understand of the organization's threat environment and take appropriate mitigation actions including real-time response.
- **Authentication management:** Government agencies should define robust management process for allocating and managing authentication information (e.g. passwords, tokens, encryption keys). This may include ensuring authentication information is strong through mechanisms such as Multifactor Authentication (MFA). Requiring multiple forms of authentication can make it much harder for hackers to gain access to sensitive data.
- **Segregation of networks:** Dividing the network within a security boundary into smaller segments can help contain breaches and prevent them from spreading. Segmentation can be based on groups of information services, users as well as business needs.

Navigating the Regulatory Landscape

Compliance isn't just a buzzword—it's a lifeline for data protection. From European Union's General Data Protection Regulation (EU-GDPR) to local data protection laws like the Kenya Data Protection Act; Computer Misuse and Cybercrime Act, etc. the regulatory landscape is complex and evolving. Government agencies must ensure that their data collection and storage practices comply with all relevant regulations. Failure to do so can result in hefty fines and damage to their reputation.

Think of encryption as the invisible shield protecting sensitive data. But not all encryption is created equal. Government agencies must stay ahead of the curve by implementing state-of-the-art encryption methods to safeguard critical information. Encryption scrambles data so that it can only be read by those with the decryption key. This makes it much harder for hackers to steal and misuse data, even if they manage to breach a system.

Empowering Citizens: Know Your Data Rights

In a democracy, power belongs to the people—and that includes power over personal data. Citizens have the right to know what data is being collected about them; how it's being used and who has access to it.

Governments should be transparent about their data collection practices and provide individuals with the tools and information they need to exercise their data rights. This includes the right to access, correct, and delete their personal data.

Risk Assessment

Predicting cyber threats might seem like fortune-telling, but with the right risk assessment strategies, it's more science than magic. Government agencies must adopt a proactive approach, constantly evaluating and mitigating potential risks. This includes identifying critical assets, assessing vulnerabilities, and developing plans to respond to breaches. By taking a proactive approach, agencies can reduce the likelihood and impact of cyberattacks.

Your Role in Ensuring Data Security

Whether you're a government employee or a concerned citizen, you play a crucial role in data security. Government employees should be aware of cybersecurity risks and follow best practices for data handling. It's important to report any suspicious activity to the ICT department or your IMS Champion and stay informed about the latest cybersecurity threats and trends.

Citizens, on the other hand, should be mindful of their digital footprint and the information they share online. Using strong passwords and enabling two-factor authentication whenever possible are essential steps. Additionally, staying informed about your data rights and holding your government accountable for protecting your personal information are key responsibilities.

Conclusion and Call to Action

KEBS has made a significant stride towards robust information security by implementing an Information Security Management System (ISMS) based on the ISO/IEC 27001 standard. This initiative underscores KEBS's dedication to safeguarding sensitive information and maintaining the trust of its stakeholders. However, in the dynamic realm of cybersecurity, continuous improvement is essential.

To further strengthen its information security posture, KEBS should focus on several critical areas. First, enhancing data privacy by developing and formalizing a comprehensive data masking policy, creating and publishing a clear, accessible data privacy policy on the KEBS website and other public-facing portals, and integrating privacy considerations into data exchange documentation.

Next, empowering through education by expanding the Security Awareness, Education, and Training program, introducing engaging, real-world scenarios like phishing campaigns as teachable moments, and ensuring strict adherence to the training schedule for all employees. Strengthening audit processes is also crucial, incorporating advanced security assessment methodologies and implementing regular Vulnerability Assessments and Penetration Testing.

Additionally, tailored security objectives should be encouraged, with individual functions within KEBS customizing their specific security objectives. This includes referencing Annex A controls for domain-specific guidance (e.g., People, Technological, Supplier, Physical, Environmental, Business Continuity) and identifying and inventorying Personally Identifiable Information (PII) processed by each function.

Through these initiatives, KEBS can create a more robust, adaptable, and effective information security framework that not only meets international standards but also ensures compliance to local regulations on data privacy protection.

CYBERSECURITY RISK AND THE ROLE OF INTERNAL AUDIT

By: Eric Kirubi – Chief Manager Internal Audit

CYBER SECURITY AWARENESS MONTH!
LET'S HELP EVERYONE BE CYBER SMART!

Introduction

Why Cybersecurity?

The rapidly evolving digital landscape has ushered in unprecedented opportunities for organizations as well as a myriad of vulnerabilities and threats. For this reason, organizations must navigate the intricate web of information security challenges to protect their information resources, including critical infrastructure. Threats to information resources may come from either inside or outside the organization

YOU KNOW, YOU COULD GET A LOT MORE OUT OF US ONLINE.
CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM

Cybersecurity refers to the technologies and processes designed to protect an organization's information resources (computers, network devices, software programs, and data) from unauthorized access, disruption, or destruction. A proactive approach to information security minimizes the risks of data breaches, unauthorized access, and potential financial and reputational damages thus fostering trust among stakeholders.

Significance of Cybersecurity Risk

How serious is Cybersecurity risk?

Organizations of all types are becoming more vulnerable to cyber threats due to their increasing reliance on computers, networks, programs and applications, social media, and data. Further, a greater variety of data has become readily available as organizations often store large volumes of sensitive and confidential information in virtualized infrastructure accessible through cloud computing.

Below are some statistics on the significance of the Cybersecurity risk from global, regional and national surveys.

a. The Global Risk in Focus 2024 Survey Results published by the Internal Audit foundation identified Cybersecurity as one of the 3 areas of highest risks affecting organizations across the world.

b. According to the State of Cybersecurity 2023, Global Update on Workforce Efforts, Resources and Cyberoperations report published by ISACA, 38% of respondents surveyed indicated that their organization was experiencing more cyberattacks than a year ago.

c. The Global Cybersecurity Outlook 2024, INSIGHT REPORT, published in January 2024 by the World Economic Forum in collaboration with Accenture had 29% of organizations surveyed reporting to have been materially affected by a cyber incident in the past 12 months.

d. Among the key findings in the African Cyberthreat Assessment Report 2024 by INTERPOL was that ransomware, business email compromise, and other forms of online scams were the most rapidly expanding threats in 2023.

e. According to the Cybersecurity Report, 34th Edition, Quarter 4 FY 2023/2024 (April-June 2024) published by the Communications Commission of Kenya, 1.1 billion cyber threat events were detected during the three-month period between April and June 2024, which represented a 16.50% increase from the 971,440,345 threat events detected in the previous period (January to March 2024).

Motives behind Cyber Attacks

Why Cyber attacks?

A motive originates from the notion that the target system stores or processes valuable information. Cyberattacks are perpetuated for varied reasons including, but not limited to;

a. Disrupting business continuity

b. Information theft

c. Manipulating data

d. Creating fear and chaos by disrupting critical infrastructures

e. Propagating religious or political beliefs

f. Achieving state's military objectives

g. Damaging reputation of the target

h. Taking revenge

To understand the cyber threats relevant to an organization, it is important to determine what information would be valuable to outsiders or cause significant disruption if unavailable or corrupted. It is also important to identify what information may cause financial or competitive loss or reputational damage to the organization if it were acquired by others or made public.

The Cyber Attack Kill Chain

How is a Cyber attack planned and intrusion executed?

Attackers try various tools and techniques to exploit vulnerabilities ina computer system or security policy and controls to achieve their motives. Understanding the multiple stages of a cyber-attack could allow information security teams to recognize, intercept, or prevent the threats as well as improve incident management and response. The following is a brief description of the seven (7) stages of a cyber attack, commonly known as the cyber kill chain;

a. **Reconnaissance-** The attacker gathers information on the target before the actual attack e.g. from publicly available information on the internet. May take hours to months.

b. **Weaponization-** The attacker uses an exploit and creates a malicious payload/malware to send to the victim e.g. PDF, MS Word, Excel etc. This happens at the attacker's side, without contact with the victim. May take hours to months.

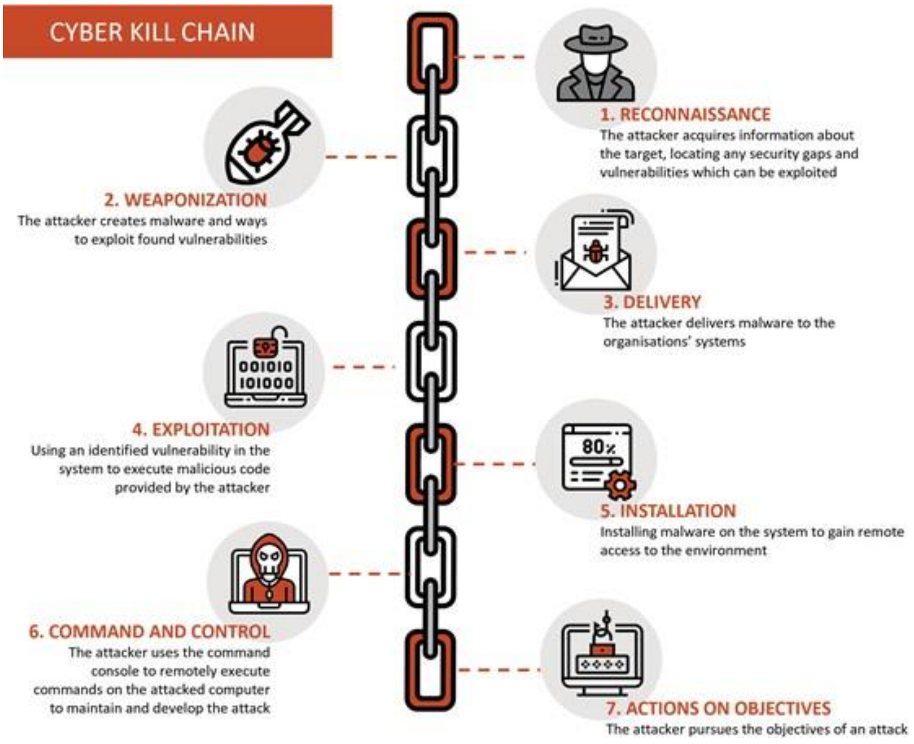
c. **Delivery-** The attacker sends the malicious payload/malware to the victim via email attachments, USB device, Web etc. This may take a matter of seconds.

d. **Exploitation-** The attacker exploits a vulnerability to execute a malicious code on victim's system. This may take a matter of seconds.

e. **Installation-** The attacker installs malware on the victim's information systems asset to gain remote access into the victim's environment. This may take a matter of seconds.

f. **Command and Control-** The attacker creates a command-and-control channel for remote exploitation of the victim. May take months.

g. **Action on objectives-** with access into the victim's network, the attacker performs the steps required to accomplish their original goals. May take months.


CYBER KILL CHAIN
1. RECONNAISSANCE
The attacker acquires information about the target, locating any security gaps and vulnerabilities which can be exploited
2. WEAPONIZATION
The attacker creates malware and ways to exploit found vulnerabilities
3. DELIVERY
The attacker delivers malware to the organisations' systems
001010
101000
4. EXPLOITATION
Using an identified vulnerability in the system to execute malicious code provided by the attacker
80%
5. INSTALLATION
Installing malware on the system to gain remote access to the environment
6. COMMAND AND CONTROL
The attacker uses the command console to remotely execute commands on the attacked computer to maintain and develop the attack
7. ACTIONS ON OBJECTIVES
The attacker pursues the objectives of an attack

Role of Internal Audit in Cybersecurity

How can the Internal Audit department assist in in the management of Cybersecurity risk?

Internal Audit plays the role of providing Senior Management and the Board with independent and objective assurance on the effectiveness of governance, risk management, and controls. **Regulation 161** of the Public Finance Management Regulations, 2015 requires Internal Auditors, among others, to comply with the International Professional Practices Framework (IPPF) as issued by the Institute of Internal Auditors (IIA) from time to time. **Standard 9.4** of the Global Internal Audit Standards (GIAS) issued by the IIA requires the Internal Audit plan to include, among others, the list of proposed engagements and related analysis, specifying the degree to which the engagements are predominately addressing financial, compliance, operational, cybersecurity, or other objectives.

According to the Global Technology Audit Guide (GTAG) issued by the IIA on Assessing Cybersecurity Risk, Internal Audit plays a crucial role in assessing an organization's Cybersecurity risks by considering the following questions;

a. Who has access to the organization's most valuable information?

b. Which assets are the likeliest targets for cyberattacks?

c. Which systems would cause the most significant disruption if compromised?

d. Which data, if obtained by unauthorized parties, would cause financial or competitive loss, legal ramifications, or reputational damage to the organization?

e. Is management prepared to react quickly if a cybersecurity incident occurred?

To effectively play this role, the IPPF requires Internal Auditors to have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

Continuous assessment of the Cybersecurity governance and controls will help in determining how risks are managed and how well corrective actions are operating. An effective assessment approach will require more than routine checklist adherence surveys. It calls for an objective and independent assurance that Management has implemented a monitoring strategy designed to generate behavioural change that includes but not limited to;

a. Access level evaluation and scanning that involves monitoring people with access to sensitive information to measure related cybersecurity risk.

b. Vulnerability assessment through regularly scanning systems to identify vulnerabilities within the environment and invoking remediation activities for identified vulnerabilities.

c. Third-party risk assessments and monitoring of the level of security risk posed to the organization based on the services provided by the third parties. For example, a vendor who hosts sensitive organizational data.

d. Penetration testing for known vulnerabilities to assess preventive technical controls, as well as management's ability to detect and respond to attacks. The tests should be reasonable in scope, approved in advance and nondisruptive to normal operations.

e. A process to regularly scan devices and products, identify vulnerabilities, and patch systems in order of priority i.e. critical assets with critical patches first.

f. Incident monitoring and response that allows an organization to detect, respond to, remediate, recover, and report to management in the event of a breach.

Logging and monitoring technologies, as well as a highly trained response team, are essential to ensure that these controls are successful in meeting their objectives.

Conclusion

So what?

Cybersecurity risks are more dynamic than most traditional risks and thus necessitate a timely response. Internal Auditors are required to ensure that management has implemented both preventive and detective controls as well as response capabilities with a focus on shortening the response time. Examples of emerging factors that calls for a comprehensive audit approach on Cybersecurity include;

a. The growing proliferation of technology enabling more user access to an organization's information.

b. A greater variety of data has become readily available as organizations store large volumes of sensitive and confidential information in virtualized infrastructure that are accessible through cloud computing.

c. Increasing number of devices that can be connected to information system assets and used in data exchange

d. Cybersecurity regulations may increase in complexity as requirements on disclosure of cybersecurity incidents or breaches continue to grow.

On the other hand, Management should design and implement effective Cybersecurity controls and governance. Strong Cybersecurity governance depends on;

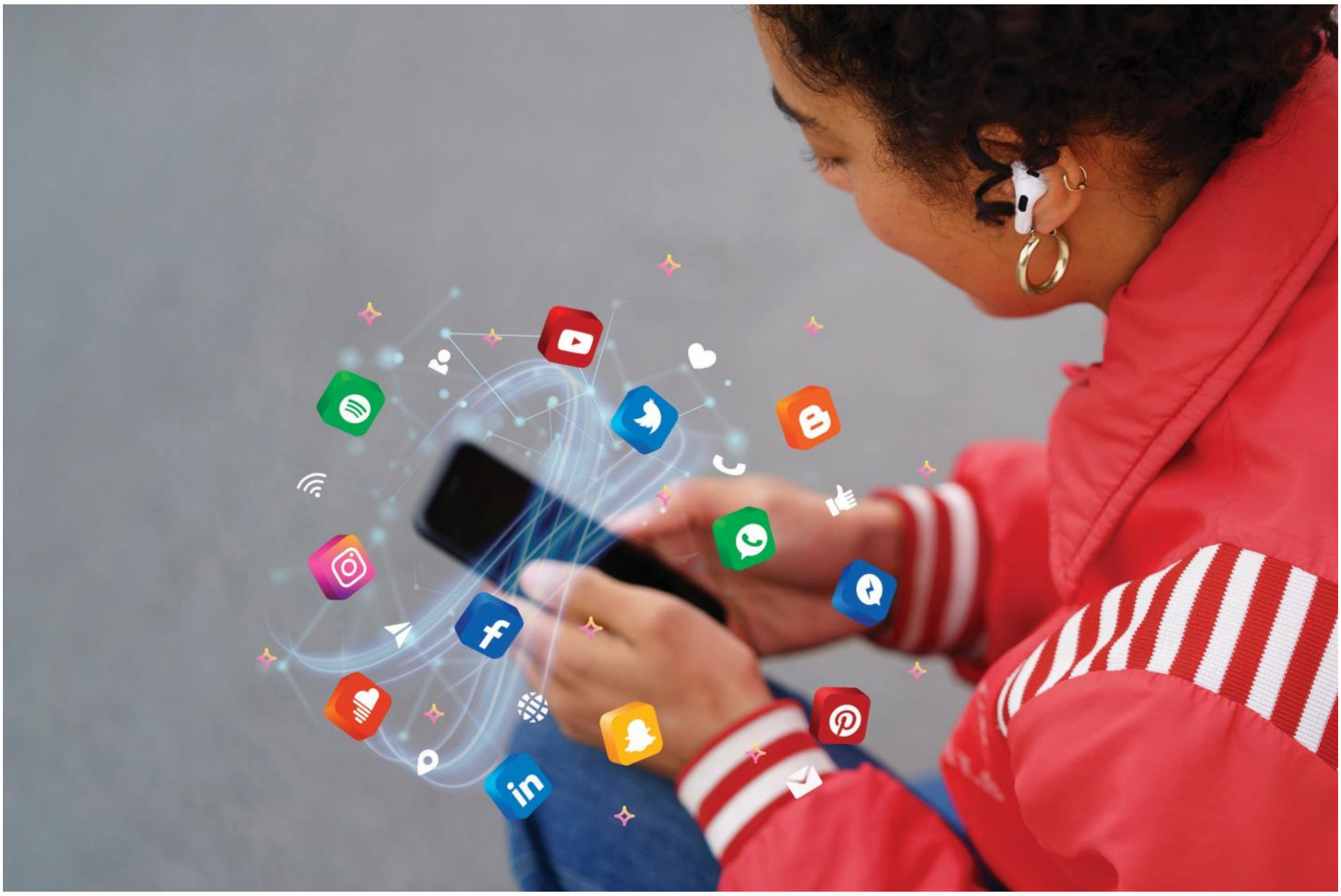
a. Collaborating and collecting cybersecurity risk intelligence and expertise based on threats that could affect the organization.

b. Setting risk appetite and tolerance levels.

c. Planning for business continuity and disaster recovery in the event of a disruption.

d. Responding promptly to information security breaches.

e. Establishing a culture of awareness of Cybersecurity risks and threats.



SOCIAL MEDIA SECURITY AWARENESS – THE DARK SIDE

Communication all over the world in the recent times has been changed by the tremendous growth of social media which has resulted into a fast-growing digital space for information sharing. Governments and private sector businesses have waded into tapping the increased usage of the digital space by way of running a digital economy.

According to Hootsuite Digital 2021 Data Report, East Africa has 20 million social media users, with Kenyans leading the pack with 11 million users. The information reported from https://www.statista.com, it indicates that, approximately 22.5 Kenyans used the internet in 2023 of which this is forecast to increase to nearly 39 million by 2028.

Social media makes it easy for everyone to connect with friends and family, and it has also fueled business growth by making it easier to target audiences with specific interests. It has therefore become an integral part of daily lives for billions of people, shaping the way they connect and communicate with each other across the urban centers to rural areas.

Nevertheless, with the widespread use of social media, it poses numerous cyber security threats including scams, malwares attack as well as cyber bullying and privacy concerns that users need to be aware of.

This article explores the dark side of social media, the potential threats it poses, and practical steps to protect yourself from cyber-attacks and maintain your privacy online:

The Hidden Dangers of Social Media

1. **Phishing Attacks:** It is an attempt to steal sensitive information where cybercriminals often leverage social media platforms to launch tricks to users into revealing sensitive information or login credentials which they later exploit for malicious gains. These attacks can occur through malicious links, fake profiles, or deceptive messages.

2. **Account Hijacking:** This is when a cybercriminal gains access to your social media account by often sending you an email with unsuspicious link that would lead you into a fake login page. It could also be an exciting storyline that requires you to login for more information. By logging in or clicking on a static video link provided, the cybercriminals steal your information and changes your credentials hence taking control of your social media profile. Once an account is compromised, cybercriminals can misuse it to spread malware, spam, or engage in fraudulent activities.

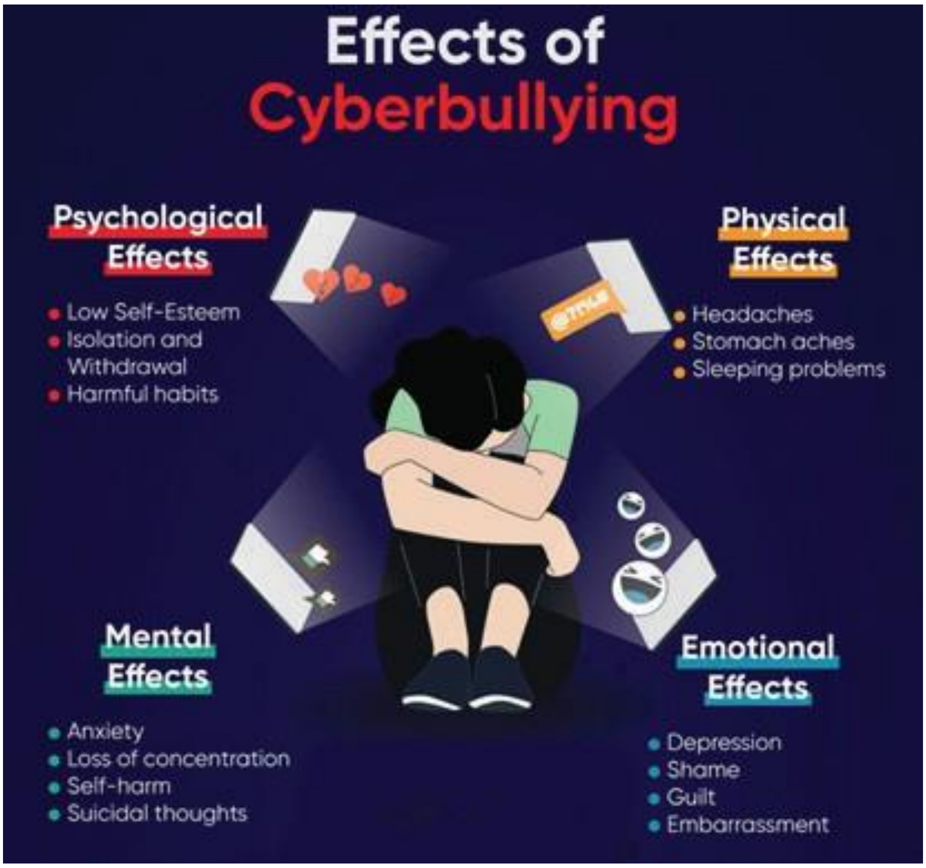
3. **Cyberbullying/Cyberstalking:** This refers to the use of electronic communication to harass, threaten, or humiliate others with the intention to harm them. In the layman terms, it could be termed as cyber harassment. Cyberstalking can be seen as an extension of the physical form of stalking but in this case sending unsolicited e-mails, including hate, obscene or threatening mail/message, which is intended to present a range of physical, emotional, mental and psychological damage on the victim.

Kenyan laws prohibit cyberbullying as captured under Section 27 of the Computer Misuse and Cybercrimes Act, 2018.

4. **Malware Distribution:** Social media platforms can be breeding grounds for malware distribution. Malicious links or downloads disguised as legitimate content can infect devices with malware, compromising security and privacy. Cybercriminals may post malicious links or apps that, when interacted with, can infect your device with malware. This malware can range from spyware and adware to more severe threats like ransomware. Social engineering has been noted to be a common way to spread malware and viruses on social media. Nearly 1 in 5 organizations worldwide are now infected by malware distributed by social media platforms.

5. **Impersonation and Identity Theft:** This is a situation where attackers create fake profiles to impersonate others on social media, often for financial gain or to damage reputations. Oversharing personal information on social media can make users susceptible to impersonation or identity theft. Cybercriminals can gather personal details and use them to impersonate individuals, commit financial fraud, or engage in social engineering attacks.

6. **Fake News and Misinformation:** Fake news can be termed as news articles that are intentionally and verifiably false and designed to manipulate people's perceptions of real facts, events, and statements. False information can influence public opinion, incite panic amongst people, and even impact on national security. Social media's rapid dissemination of information makes it a powerful tool for spreading misinformation and fake news to unsuspecting audience. According to DeepMedia, in 2023, roughly 500,000 video and voice deepfakes were shared on social media around the world.



How to stay secure in Social Media platforms

Understanding the benefits of social media security is a good starting point for both individuals and businesses alike to ensure a safer and more secure online presence.

1. **Use strong, unique passwords:** Use strong, unique passwords for each social media account. Avoid reusing passwords across platforms and consider using a password manager to securely store and manage your credentials

2. **Enable multi-factor authentication (MFA):** Enable multi factor authentication for your social media accounts whenever possible. This adds an extra layer of security by requiring a secondary verification method, such as a code from a mobile app or a text message.

3. **Be cautious about sharing personal information:** Be selective about the personal information you share on social media and avoid

posting sensitive details such as your address, phone number, or financial information.

4. **Regularly Monitor and Review Account Activity:** Regularly monitor your social media accounts for any suspicious activity, such as unauthorized login attempts or unusual posts. Report any suspicious activity to the platform and take appropriate action to secure your account.

5. **Beware of phishing scams:** Be cautious when clicking on links or downloading attachments from unknown sources. Never entertain strangers engaging you with personal questions. Clicking on links that appear in random emails and instant messages, however, isn't such a smart move. Hover over links that you are unsure of before clicking on them to see if they lead where they are supposed to lead. A phishing email may claim to be from a legitimate company and when you click the link to the website, it may look exactly like the real website

6. **Avoid public Wi-Fi** Avoid public Wi-Fi connections as much as possible, like those offered at coffee shops or airports, when using a website that asks for a password. Limit your social media usage to personal or private Wi-Fi networks, while using cellular data on your phone, or under the protection of a Virtual Private Network (VPN).

7. **Become aware:**

- Adjust your privacy settings regularly to control who can see your information.
- Be cautious about the personal details you share online and verify the identity of people you meet online before engaging in financial transactions.
- Verify news from reputable sources before sharing it.
- Be skeptical of sensational headlines and stories
- Enable account recovery options to regain access quickly if hacked
- Familiarize yourself with the privacy policies of social media platforms you use. Understand how your data is collected, stored, and shared, and make informed decisions about the platforms you engage with

KEBS
Kenya Bureau of Standards
Standards for Quality life
SECURE OUR WORLD
1923
2014
01 FACEBOOK ADS
Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat.

THEY LOOK FRIENDLY | BUT THEY'RE NOT

"DON'T TRUST ANONYMOUS FACEBOOK REQUESTS; THEY OFTEN TURN OUT TO BE SCAMS"

- Report suspicious messages to facebook by Tapping the 'something's wrong' button.
- IF you receive a suspicious email from face- book, forward it to phish@fb.com.
- Block, report, ignore, or delete any suspicious facebook requests or messages
- IFyou suspect that an account is fake or impersonating someone, report it.

#CYBERSECURITY AWARENESS MONTH

Pictorial

Members of the National Standards Council led by the Chairman, Anthony M. Munyiri (centre), joining the Head of Public Service, Felix Koskei (3rd right) during a cake cutting moment during celebrations to mark World Standards Day, which coincided with KEBS' 50th Anniversary commemorations. They are from left, Momanyi Nyabonyi, Patricia Okune, Musa Osman and Stephen Kipkosgei. Other in the picture are the Cabinet Secretary in the Ministry of Investment, Trade and Industry, Salim Mvurya (4th from right), KEBS Managing Director, Esther Ngari (2nd from right) and Principal Secretary for Industry in the Ministry of Investment, Tade and Industry, Dr. Juma Mukhwana extreme (right).

Head of the Public Service, Felix Koskei, signs the visitors' book when he arrived at the Kenya Bureau of Standards to celebrate the World Standards Day, and KEBS' 50th anniversary.

National Standards Council Chairman, Anthony M. Munyiri, addresses celebrations to mark the World Standards Day, and to commemorate Kenya Bureau of Standards' 50th anniversary.

National Standards Council Member, Wabwile Kennedy Simiyu, while attending this year's World Standards Day celebrations at the Kenya Bureau of Standards, which also coincided with the celebrations to mark KEBS' 50th anniversary.

National Standards Council Members Francis Kuria Karu (left), and Stephen Kipkosgei Yego during the World Standards Day celebrations at the Kenya Bureau of Standards.

KEBS' CELEBRATES 50 YEARS OF CONSUMER PROTECTION AND QUALITY ASSURANCE

A section of Kenya Bureau of Standards' staff following the proceeding during celebrations to mark the World Standards Day, and to commemorate KEBS' 50th anniversary.

Several organizations were awarded the ISO 9001;2015, Quality Management System Certification during this year's World Standards Day. Here, the Engineers Board of Kenya led by the Chairman, Eng. Erastus Mwongera (extreme left), while receiving their certification from the Head of the Public Service, Felix Koskei (3rd left).

Kenya Bureau of Standards Legal Services and Corporation Secretary, Miriam Boit Kahiro, follows the proceedings during celebrations to mark this year's World Standards Day during which KEBS commemorated its 50th anniversary.

The Principal Secretary in charge of Industry at the Ministry of Investment, Trade and Industry, Dr. Juma Mukhwana, while addressing this year's World Standards Day which coincided with celebrations to mark the 50th anniversary of the Kenya Bureau of Standards.

Kenya Bureau of Standards Managing Director, Esther Ngari, while addressing this year's World Standards Day celebrations at the KEBS' Headquarters. KEBS also commemorated its 50th anniversary during the occasion.

Head of Public Service, Felix Koskei, plants a commemorative tree when he arrived at the Kenya Bureau of Standards to lead celebrations to mark this year's World Standards Day, and to commemorate KEBS' 50th anniversary.

Happiness is not a matter of intensity but of balance,
order, rhythm, and harmony.

Thomas Merton

WAJIBIKA NA KEBS

www.kebs.org

Kenya Bureau of Standards
Standards for Quality life

YEARS OF SAFEGUARDING GENERATIONS

A Legacy of Quality On this World Standards Day 2024, we honor KEBS' half-century of promoting standardization in industry and commerce. KEBS ensures consumer health, safety, and environmental protection, marking a legacy of quality.

EDITORIAL TEAM: Managing Editor: Verah Akomo **Content Editor:** Geoffrey Nyerere,

Editorial Consultants: Humphrey Odhiambo, Solomon Kyenze, **Content contributors:** Urbanus Kissiu,

The Kenya Bureau of Standards monthly newsletter is designed by The ARCrayon Limited

For feedback, queries or comments, please contact the communications office via Email: communications@kebs.org | Tel: 020 6948458/265
Toll Free Number - 1545

www.facebook.com/kebs.org KEBS_ke Kenya Bureau of Standards www.kebs.org Kenya Bureau of Standards

SM#20023