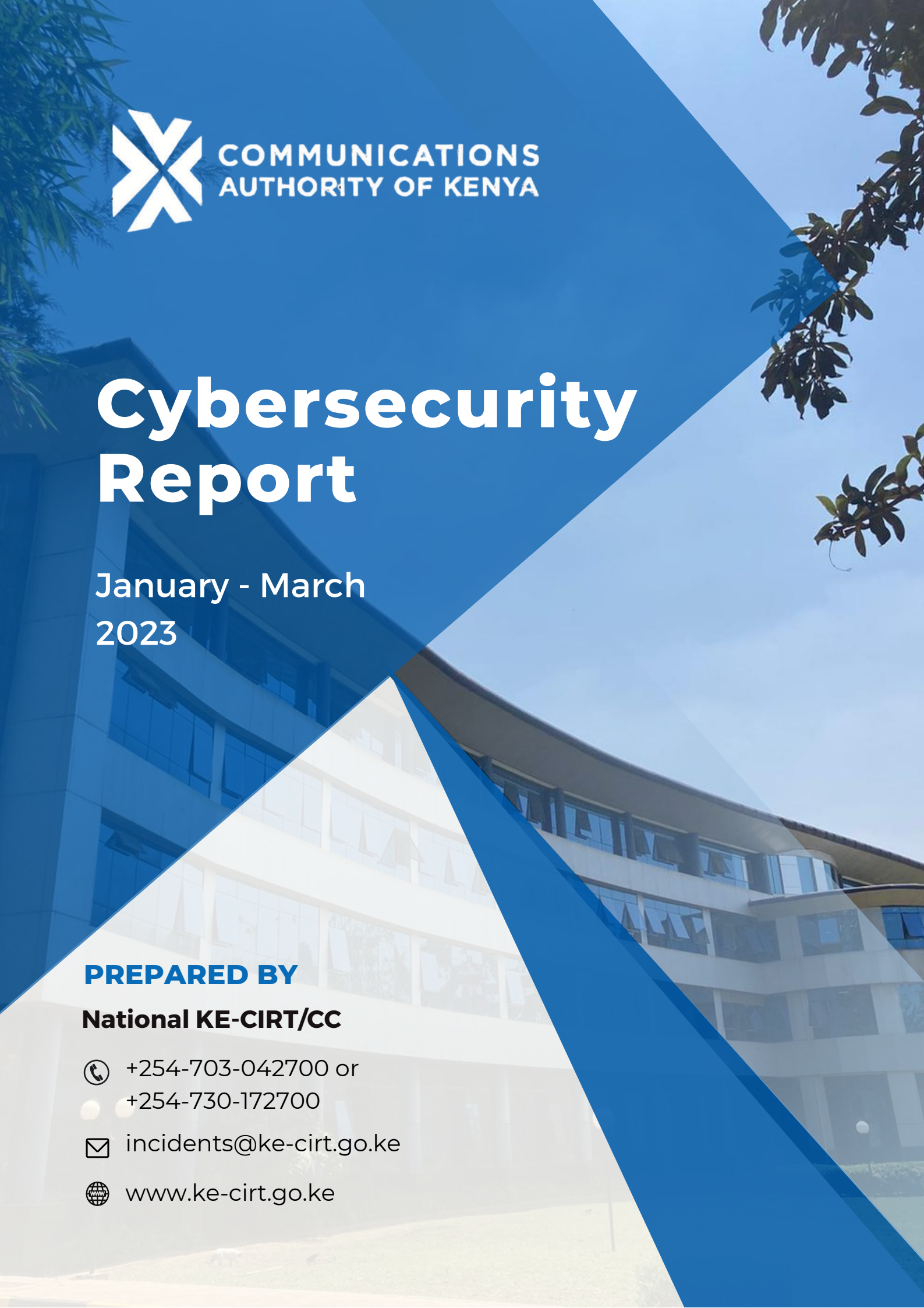


COMMUNICATIONS AUTHORITY OF KENYA

Cybersecurity Report

January - March 2023

PREPARED BY

National KE-CIRT/CC

+254-703-042700 or
+254-730-172700

incidents@ke-cirt.go.ke

www.ke-cirt.go.ke

Our Vision

A Digitally Transformed Nation.

Our Mission

Building a connected society through enabling regulation, partnership and innovation.

Cybersecurity Mandate

The Kenya Information and Communications Act, 1998, mandates the Communications Authority of Kenya (CA) to develop a framework for facilitating the investigation and prosecution of cybercrime offenses.

It is in this regard, and in order to mitigate cyber threats and foster a safer Kenyan cyberspace, that the government established the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC).

The National KE-CIRT/CC is a multi-agency collaboration framework that coordinates response to cyber security matters at the national level in collaboration with relevant actors locally and internationally. The National KE-CIRT/CC, which is based at the CA Centre Nairobi, comprises of staff from the Communications Authority and law enforcement agencies.

The National KE-CIRT/CC detects, prevents and responds to various cyber threats targeted at the country on a 24/7 basis. It also acts as the interface between local and international ICT services providers whose platforms are used to perpetrate cybercrimes, and our Judicial Law and Order Sector which investigates and prosecutes cybercrimes. The enactment of the Computer Misuse and Cyber Crimes Act of 2018 has further enhanced the multi-agency collaboration framework.

Director General's Perspective

The digital space is marked by rapid technological advancements that seek to deliver seamless digital experiences. This is in line with making digital transformation a meaningful, seamless, profitable and inclusive reality that spurs sustainable social economic development.

This social economic development brought about by digital transformation must encompass all. Indeed, this year's International Women's Day (IWD) 2023 commemorations were held under the theme: *DigitALL: Innovation and Technology for Gender Equality*. As the ICT sector regulator, we are cognizant of the critical role that women play in the ICT space, and acknowledge that there exist inequalities in the access to and use of ICTs, as well as the inequality in the impact of online harms between genders. To address these inequalities, the Authority has put in place various continuous programs to bridge this gap and empower women and girls to effectively participate in an equitable, thriving and safe digital nation.

On the global front, cyber threat actors are taking up even more advanced attack techniques and using increasingly sophisticated tools for purposes of compromising individuals' and organisations' digital security. In the period January to March 2023, the National KE-CIRT/CC detected *187,757,659* cyber threats targeted at various key organisations in the Country. In addition, we continued to receive complaints from the public that ranged from identity theft, online fraud, to defamation online.

"..social economic development brought about by digital transformation must encompass all."

This reality calls for a review of our current cybersecurity approaches as well as the strengthening of our individual and collective cyber defences against these rising cyber threats.

Digital transformation must therefore be accompanied by strategies to ensure the sustainability of the gains made so fair in ICTs. In line with this, the Authority held a series of engagements with various stakeholders with regard to the roll out of the National Public Key Infrastructure (NPKI) in the country.

The NPKI refers to various tools and processes that enable users to securely transact online. Through the NPKI, users are assured that the data they send or receive online is secured, and they are able to verify and authenticate the identity of transacting parties. The NPKI thereby performs a critical function in a digital economy by assuring the safety and integrity of electronic transactions and online services. The rollout of the NPKI will further enhance online service delivery through e-government, e-commerce, e-health, e-tax, e-insurance, e-learning among others. The rollout of the NPKI will also ensure that Kenya fully benefits from the gains made in ICTs, while being responsive to the latest security demands with regard to electronic transactions.

The Authority's role in the roll out of the NPKI involves licensing and regulating Electronic Certification Service Providers (E-CSPs) as provided for under the Kenya Information and Communications Act (KICA) of 1998.

As we collectively work towards building a thriving and secure digital superhighway, I wish to remind each one of us that trusted networks and collaboration are a proven critical strategy in strengthening the collective cyber readiness and resilience. It is only by leveraging on the synergies brought about by partnerships, that we can effectively defend, respond to and recover from increased cyber threats.

Ezra Chiloba
Director General

Cybersecurity Concerns around the Globe

Ransomware

Ransomware continues to be a major cybersecurity challenge as cyber threat actors adopted a range of increasingly sophisticated tactics and advanced exploit kits to carry out mass ransomware attacks.

Cyber threat actors are propagating and modifying various ransomware strains for purposes of data extortion that is increasingly being targeted at critical infrastructure. These are used to encrypt victims' files, while using advanced techniques to hide their files and processes from anti-debugging and security software. This has increased the level of difficulty in developing decryption tools by cyber security researchers, further complicating recovery and business continuity efforts.

To safeguard against ransomware threats, it is important to keep all software up to date; prioritise remediating known exploited vulnerabilities; perform regular backups; create awareness to empower users to identify and report phishing attempts; implement multi-factor authentication; and implement comprehensive ransomware response plans.

"Ransomware is not only about weaponizing encryption, it's more about bridging the fractures in the mind with a weaponized message that demands a response from the victim."

— James Scott, Senior Fellow, Institute for Critical Infrastructure Technology

Cybersecurity Concerns around the Globe

Insider Threats

An insider is any person who has access to relevant company data and computer systems such as employees, former employees, vendors or contractors.

An insider threat is a perceived cyber threat to an organisation that comes from within the organisation such as from employees; former employees, contractors, vendors, or business associates who have access to information regarding the organisation's cyber security practices, data and computer systems.

An insider can become an insider threat either intentionally or unintentionally. The unintentional insider threat occurs majorly due to poor cyber hygiene practices, for example, when a threat actor tricks them into clicking a malicious phishing link.

On the other hand, the intentional insider threat becomes so by choice, oftentimes exfiltrating company data, giving threat actors access to the organisation's critical systems, or even selling credentials and sensitive data to malicious actors. The intentional insider threat does so because they believe the organisation has wronged them, or as an act of activism.

Intentional insider threats are often passionate and motivated employees, who started out dedicated to the organisation and its mission, but due to some perceived wrong, decide to turn against the organisation.

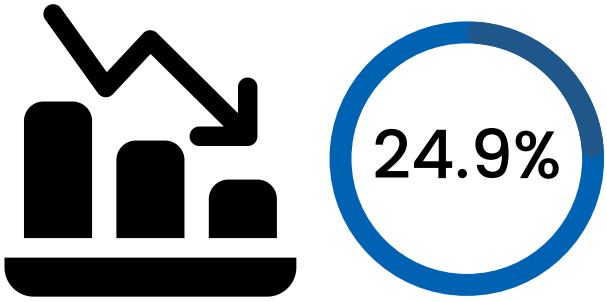
While it is difficult to predict if and when loyal employees or vendors become intentional insider threats, paying attention to possible triggers and drivers such as threats of layoffs, financial duress, as well as recurring expressed dissatisfaction with the organisation or its policies could be a warning sign.

In view of this, it is important that organisations carry out regular cyber risk assessments and implement comprehensive access control and security measures to mitigate the impact of insider threats.

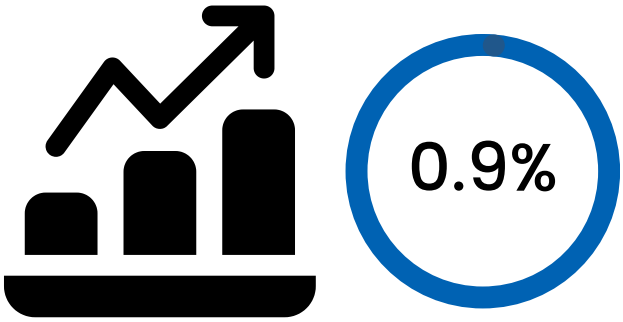
What are a CISO's two biggest cybersecurity fears?
Everyone who works at the company... and everyone who doesn't.

~(Unknown)

Cyber Threat Landscape Statistics



During the period January to March 2023, the National KE-CIRT/CC detected 187,757,659 cyber threat attempts targeting critical infrastructure service providers.
This represented a 24.89% change from the last period.



During the period January to March 2023, the National KE-CIRT/CC issued 3,584,966 cyber threat advisories to critical infrastructure service providers. This represented a 0.87% change from the last period.

% Change in cyber threat attempts detected by the National KE-CIRT/CC from the previous period (Oct-Dec 2022)

24.89%

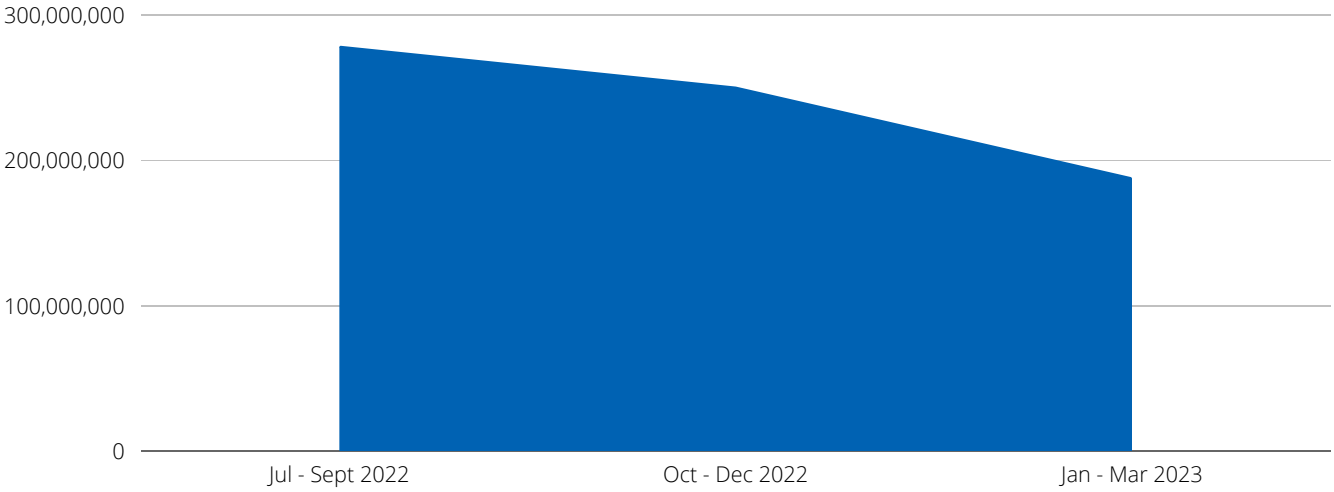
% Change in cyber threat advisories issued by the National KE-CIRT/CC from the previous period (Oct-Dec 2022)

0.87%

Cyber Threat Landscape Trend Analysis

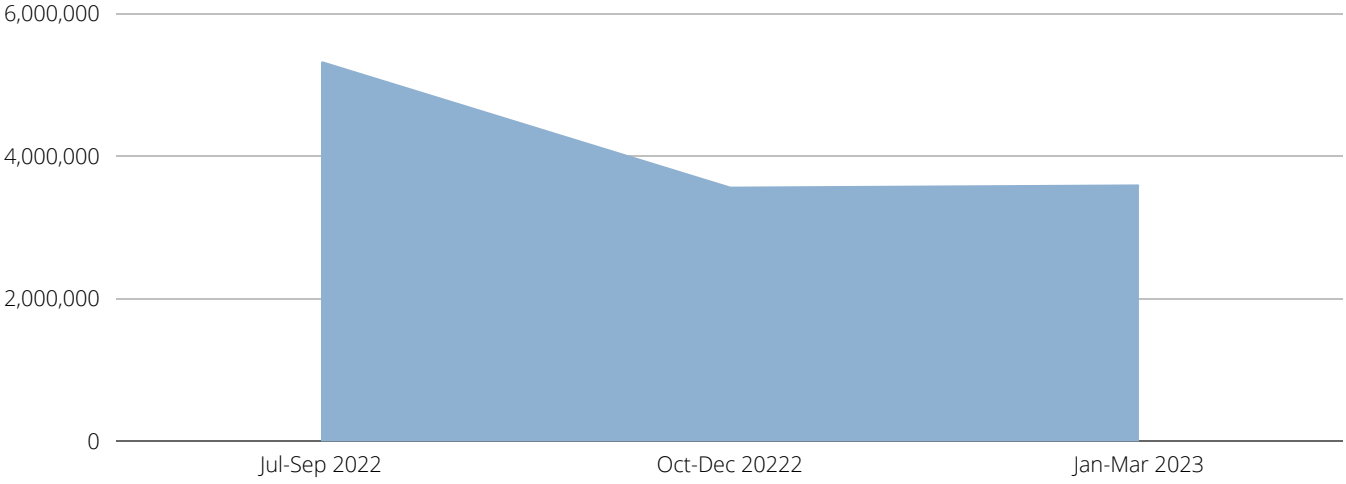
During the period January - March 2023, the National KE-CIRT/CC detected 187,757,659 cyber threat events, which was a 24.89% decrease from the 249,991,852 threat events detected in the previous period, October - December 2022.

This trend in cyber threat events detected is attributed to the continued activity by organised cybercrime groups; adoption of more sophisticated tools by ransomware gangs; continued targeted attacks at critical systems and services; adoption of sophisticated phishing and malware kits by threat actors; continued targeted attacks at cloud-based supported services and unsecured infrastructure; continued network misconfiguration attacks; and continued adoption of botnet and Distributed Denial of Service (DDoS) attack techniques.



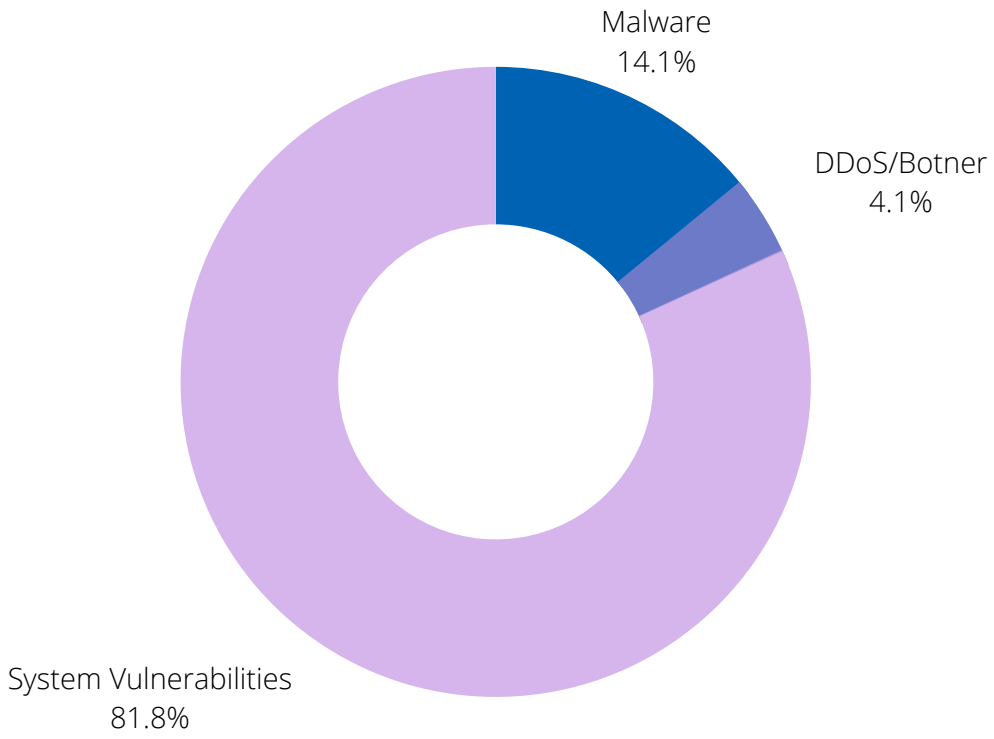
To address these emerging concerns, the National KE-CIRT/CC continued to issue Technical Cybersecurity Advisories to organisations and Cybersecurity Best Practice Guides to the public, which provided detailed insights to assist in cyber threat prevention and detection.

These included 3,584,966 advisories marking a 0.87% increase from the 3,553,999 advisories, which were shared during the period October - December 2022.



Cyber Attack Vector Trends

Insight into cyber threat vector trends during the period January to March 2023:

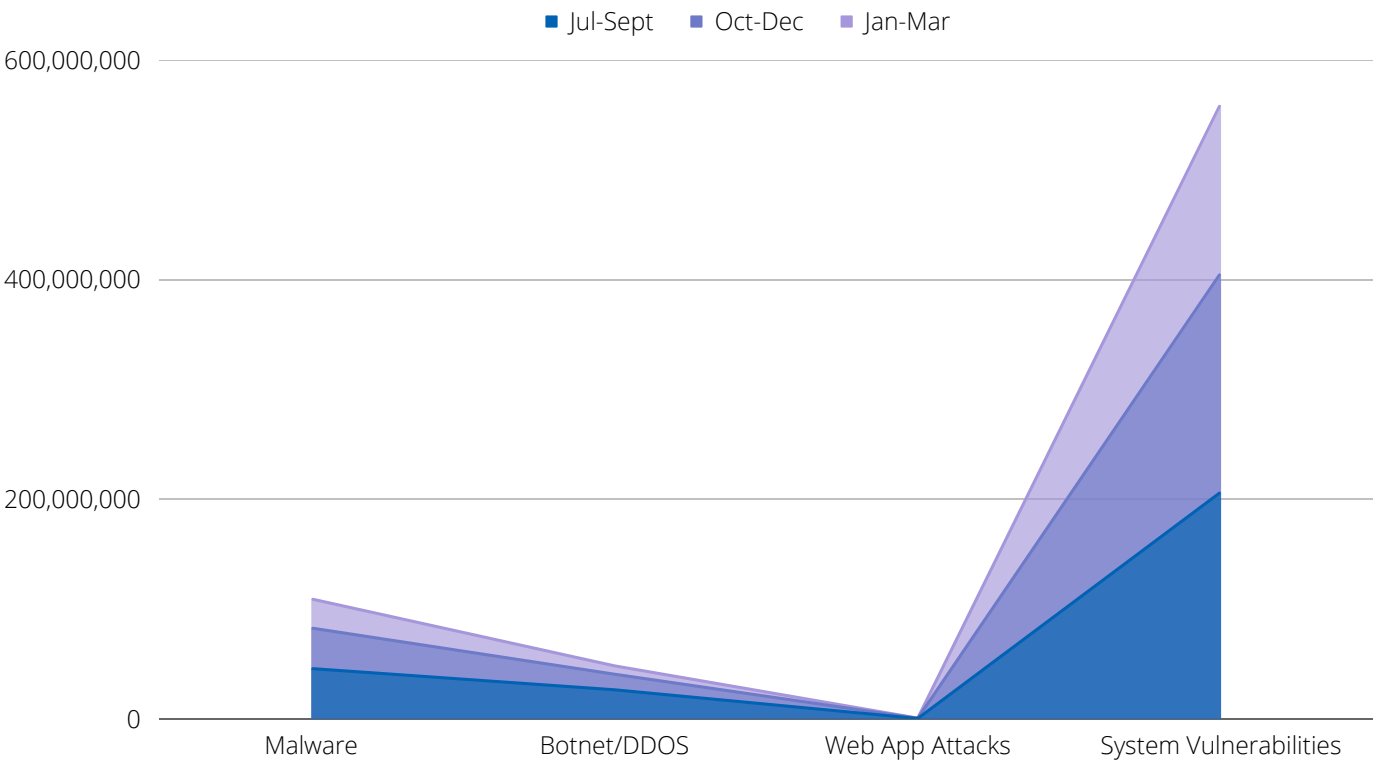


During this period, the following were notable cyber attack vector trends:

- Persistent system misconfiguration attacks
- Decrease in DDoS attacks

Cyber Attack Vector Trend Analysis

Trend analysis of cyber attack vectors used to target critical information infrastructure service providers as detected by the National KE-CIRT/CC from July 2023 to date.

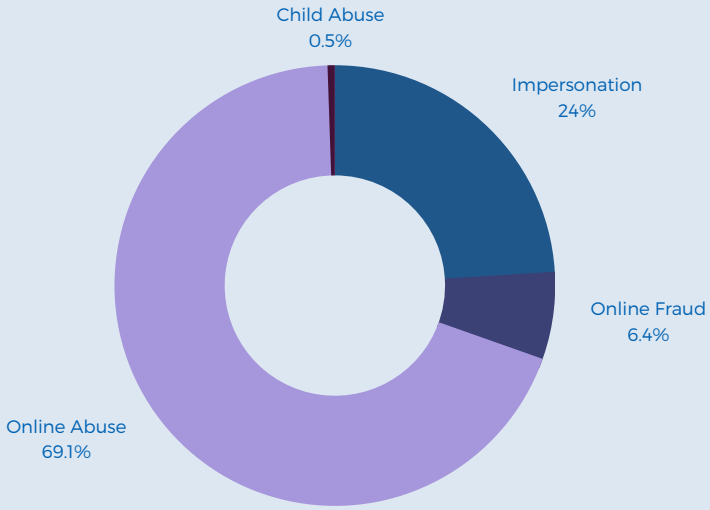


The following are the cyber threat vector trends over the past 9 months:

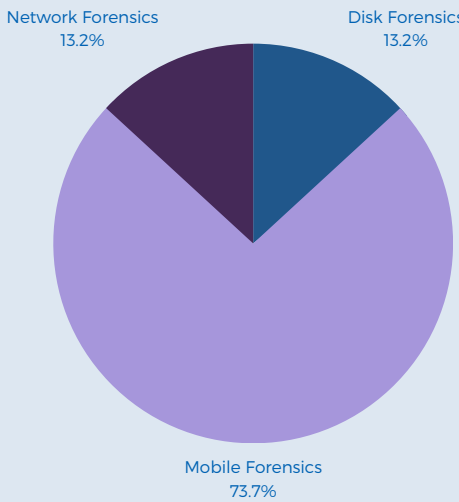
- Malware and system misconfiguration attacks continued to top the threat vectors over the past 9 months as cyber threat actors adopted sophisticated techniques to extend their attacks.

Overview of Digital Forensics & Investigations

During the period January - March 2023, the National KE-CIRT/CC received 375 digital investigation requests, which was a 24.58% increase as compared to 301 requests in the previous period.

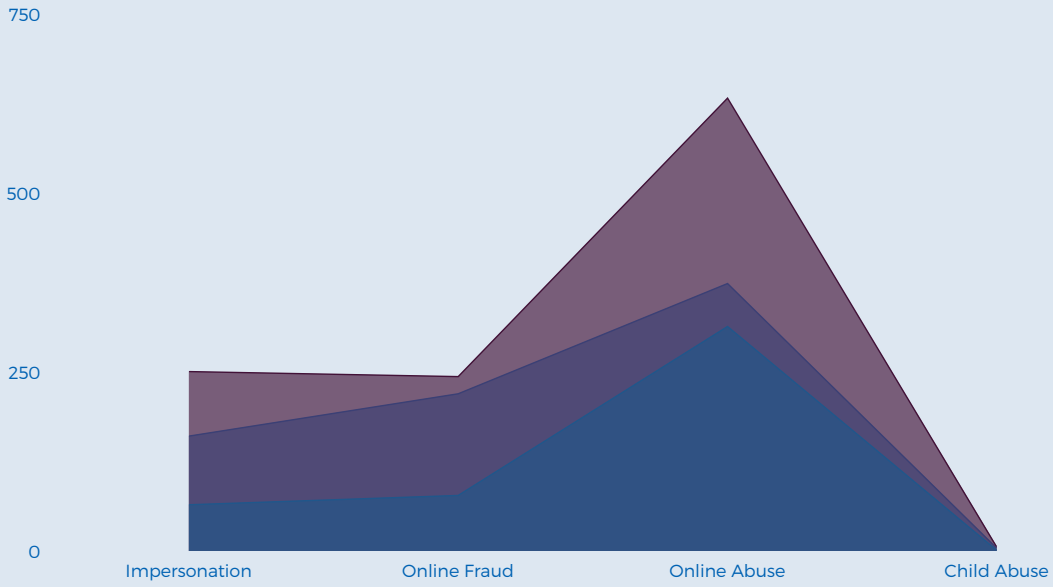


The National KE-CIRT/CC Digital Forensics Lab (DFL) carries out mobile forensics, disk forensics, and network forensics. In the period January - March 2023, the National KE-CIRT/CC Digital Forensics Lab received 38 forensic requests, which was a 32.14% decrease compared to 56 requests received in the previous period October - December 2022.

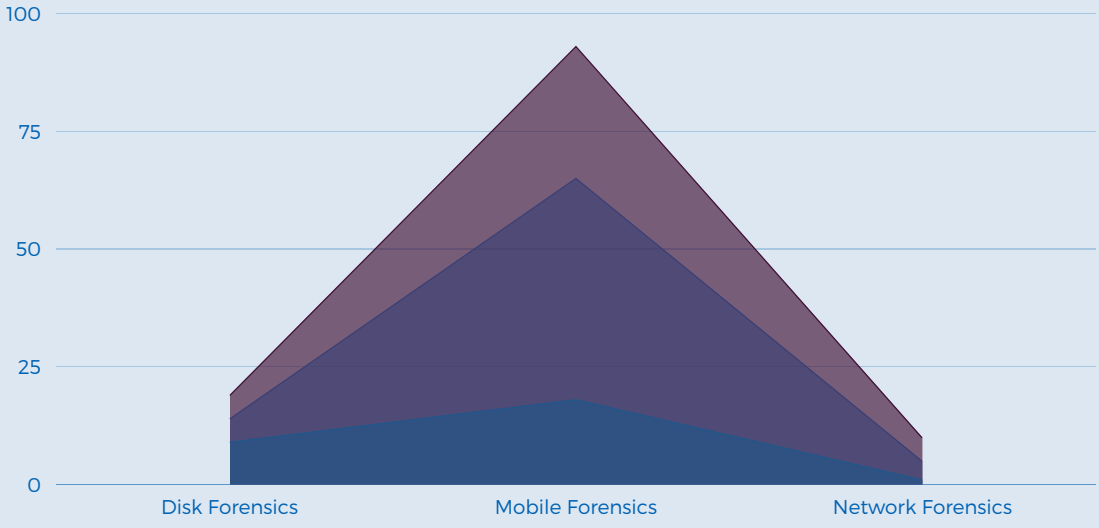


Digital Forensics & Investigations Trends

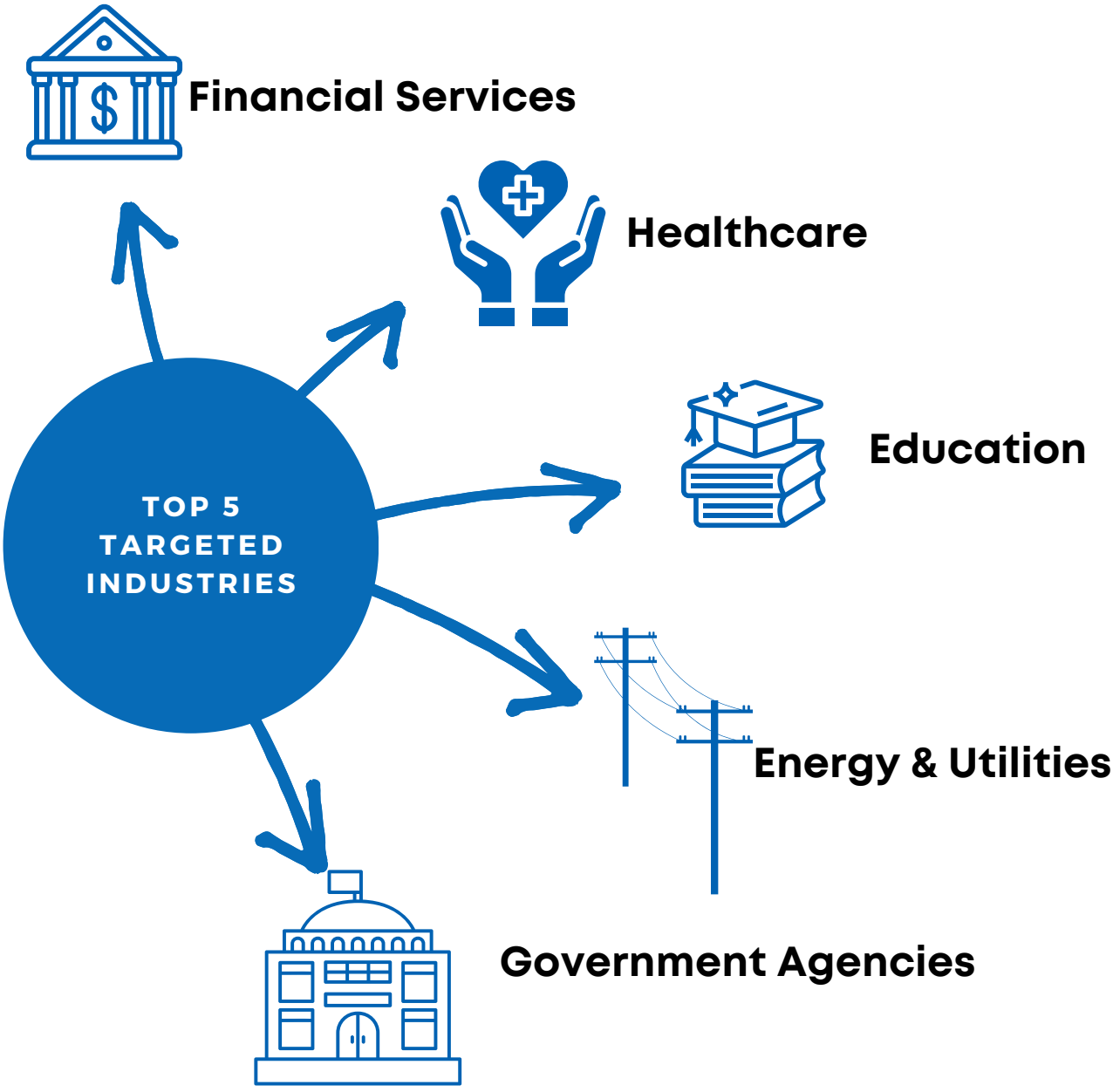
The National KE-CIRT/CC has facilitated 1,135 digital Investigations through the Digital Forensics Lab over that last 9 months starting July 2022 to March 2023.



The National KE-CIRT/CC has facilitated 122 digital forensics through the Digital Forensics Lab over that last 9 months starting July 2022 to March 2023.



Cyber Threat Trends by Sector



What is being targeted?

- Personally Identifiable Information (PII)
- Intellectual property
- Financial gain (monetary)
- Control

Impact of Cyber Attacks

01 Data Loss/ Exfiltration

Organisations continue to feel the financial pinch of recovering from data loss where legal remedies impose heavy fines for non-compliance and to compensate victims.

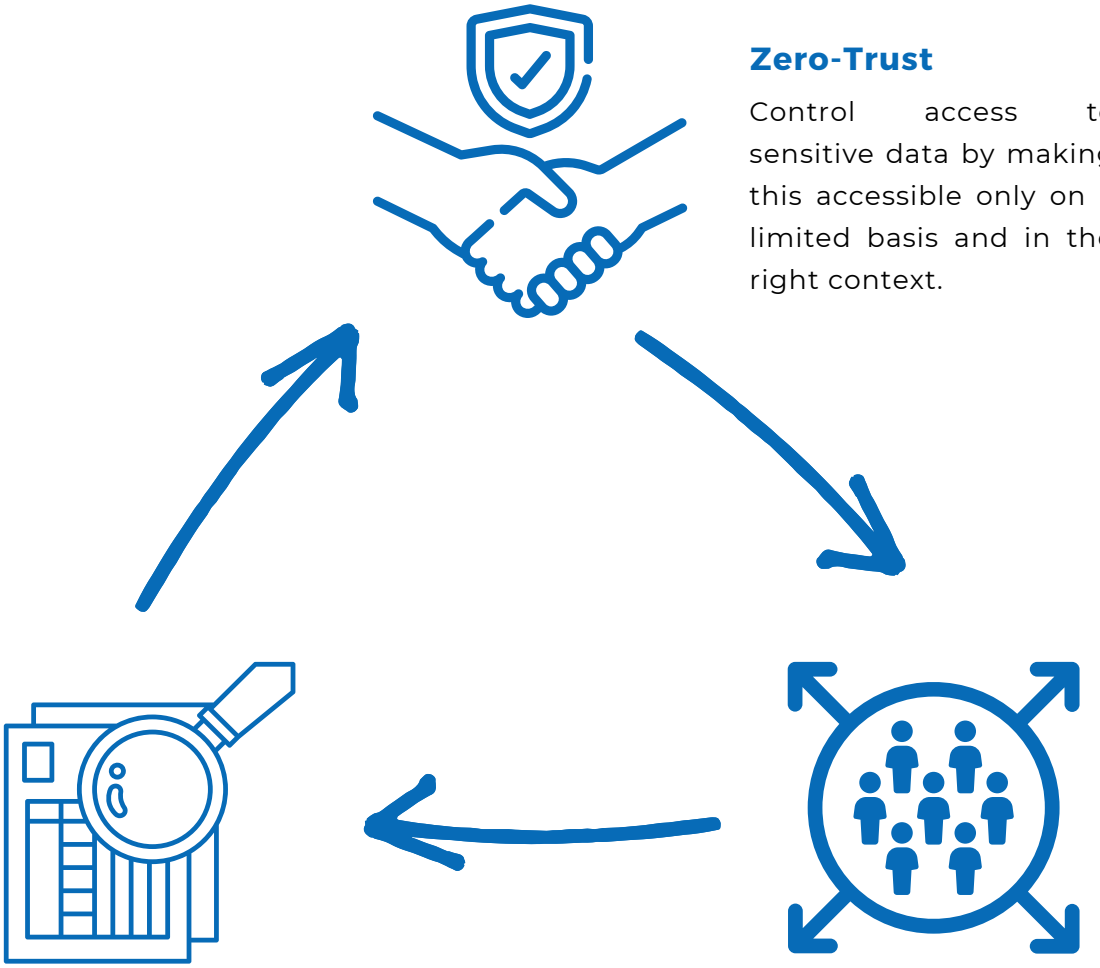
02 Reputation Loss

Trust in organisations' brands is compromised thereby disrupting business process life cycles.

03 Disruption of Services

Disrupted access to critical systems and services result in financial loss and loss of users' trust in service reliability.

Enhancing Organizational Cyber Readiness



Zero-Trust

Control access to sensitive data by making this accessible only on a limited basis and in the right context.

Cyber Drills

Cyber drills test an organisation's cyber readiness by measuring your ability to detect and respond to a cyber incident. Stress-testing your incident response plan enables you to assess the effectiveness of your overall IR plan, as well as identify gaps in awareness and preparedness of staff.

Cyber Awareness

It is critical that organisations invest in cybersecurity awareness training for all members of the team. This awareness training includes informing staff of emerging cyber threats targeted at your organisation and sector, how to identify these threats and how to protect themselves. Cyber awareness should also extend to your customers and constituents, and should include information on emerging attack vectors as well as reporting mechanisms.

Children & the Internet:

Addressing Child Online Sexual Exploitation & Abuse

Children continue to benefit from the gains realised in the move towards digitisation. This includes the opportunity to learn, interact and innovate towards reaching their full potential.

However, as more children have access to digital technologies, predators have also doubled their online efforts at targeting this vulnerable group.

A survey carried out by the Authority indicates that 64% of children aged between 11 and 17 years are exposed to various online risks such as cyber bullying, sextortion, sexting, online grooming, online sexual harassment and exposure to harmful online content through social media platforms, private chat room applications and browsers not running on safe browsing. There are significant and long-lasting impacts of these online harms on children, such as psychological harms, physical harms, self-esteem issues and sometimes, even death.

For more information on cybersecurity best practices, please visit: https://cop.ke-cirt.go.ke/

In view of this alarming trend, the National KE-CIRT/CC continues to support the investigation and prosecution of cybercrimes targeted at children, as well as working closely with agencies involved in the various aspects of Child Online Protection (COP). These efforts are geared at promoting awareness on COP; educating the public on online harms targeted at children; empowering parents and guardians with the knowledge and tools to safeguard children online; as well as empowering children to practise online safety through behavioural change campaigns.

The quest for safe digital experiences for children is a global concern that requires the concerted efforts of parents and guardians, as well as the public sector and private sector. It is important that we continue empowering children to take up cyber hygiene best practices that will enable them to safely navigate the digital space safely without fear of exploitation or abuse.

Hacking the Human

The Paradox of Progress

"How quickly we embrace novel technology is the new flex.."

It is an irrefutable fact that technology has changed humanity.

Technology has not only changed how we work, interact, or even go to war: but it also colours our perspectives of reality; shapes our value systems; it is the window through which we evaluate our lived experiences; and has an increasing impact on our hopes, dreams, and fears at individual, community, and global level.

Naturally, as humanity embraces the efficiencies and effectiveness brought about by technologies, we drive a collective need, maybe even demand, for more seamless, integrated, sleeker, shinier, autonomous, futuristic, mind boggling new tech.

We want technology that we do not even realise we need. It's the chicken and egg paradox all over again. Which comes first, the need or the tech? We can no longer be sure. The result? Tech companies are competing to make the biggest return on investment to their shareholders by leveraging on our tech dependence to ostensibly meet our unspoken demands for unconscious tech needs.

And so, every day, we are being bombarded with the latest updates, devices, and solutions that are meant to elevate our tech experience and purportedly, make our lives better.

The human loves this, embraces this, and quickly upgrades and adopts this new tech, whether it's a new gizmo, new solution or new device.

How quickly we embrace novel technology is the new flex.

Undoubtedly, our digital reality causes a few paradoxes. The first, the cybersecurity risk paradox. As societies become increasingly dependent on ICTs to drive social, economic, and even national development agendas; there is a direct correlation between their digital transformation and an increase in the magnitude, type and sophistication of cyber threats and cyber-attacks to both individuals and organisations.

In addition, the competition amongst tech companies to release the latest tech fastest, oftentimes results in security taking a backstage. This means that we could be walking around with the latest tech whose security features were a secondary consideration during development.

At the organisational level, we see this through the updates by the National KE-CIRT/CC highlighting hundreds of millions of cyber-attacks targeted at critical infrastructure service providers. These include millions of attempted cyber-attacks at key services such as utility providers (water and power), health care, manufacturing, telecommunications, transport services, amongst others.

At the individual level, we have millions of unreported cyber-attacks targeting our mothers, partners, children, the youth, and other vulnerable demographics online.

"It is an irrefutable fact that technology has changed humanity."

"How quickly we embrace novel technology is the new flex.."

At the heart of these cyber-attacks targeted at individuals, is the paradox of hacking the human, otherwise referred to as social engineering. For instance, smishing attacks might look like “usitume kwa hii namba, tuma kwa hii +2547xxx”, or phishing emails that take the form of congratulatory messages for jobs not applied for, or fund receipts for monies not requested.

Hacking the human involves identifying and leveraging on the human psyche; on our hopes, our fears, our dreams, our aspirations, our value systems, amongst others. It is about peeling back the layers to reveal an individual's utmost vulnerability, and leveraging on this to initiate and spread cyber-attacks.

These vulnerabilities may sometimes take the form of the quest for financial security peppered generously with our undying belief in the power of miracles. The result, a human hack in the form of phishing emails promising a quick financial return if only the recipient would “... fill in some personal details on the accompanying link, or share bank or digital wallet details... or send the link to three other people...”. Should you take the hook, the criminal on the other end will take the personally identifiable information (PII) shared and use this for fraudulent purposes.

Or it could be the quest to find that special person who will love us and complete us, that opens the door for cat-fishing on dating and social media platforms. The result? We end up still alone and lonely, but with our funds drained and emotionally manipulated.

Maybe more worrying, is how the human need for association, validation and acceptance opens the door for the online groomers and recruiters to prey on our children and the youth, taking them down the road of sexual exploitation and recruitment into radical groups.

Again, it is our inherent human bias that opens the door for malicious actors to manipulate our realities and through disinformation and cyber propaganda campaigns.

In all these scenarios, the paradox of progress that we grapple with is to endeavour to balance progress in the ICT space, with consumer empowerment and protection.

As the National KE-CIRT/CC, we recognize the need for deeper conversations and considerations on how to educate and empower ICT consumers with the knowledge, skills and values to safely navigate and thrive in the digital space.

This calls for each and every one of us in the cybersecurity community to embody Online Safety Ambassadorship in our collective spaces. For indeed, in the face of increased digital acceleration towards a digitally transformed nation, we must all rise up as the Cyber Safety League, proudly wearing our Online Safety Capes to support our communities in the safe use of digital technologies.

"Hacking the human involves identifying and levergaing on the human psyche; on our hopes, our fears, our dreams, our apirations.."

Thank You

We're here to help. Report an incident.

Working round the clock to safeguard Kenya's cybersecurity landscape.

Email
incidents@ke-cirt.go.ke

Hotlines
+254 703 042700
+254 730 172700

Website
www.ke-cirt.go.ke