SERIANU

KENYA CYBER SECURITY REPORT 2015

Achieving Enterprise Cyber Resilience Through Situational Awareness

PKF

USIU AFRICA
United States International University-Africa

Acknowledgement

Authors

Paula Musuva Kigen | Research Associate Director, Centre for Informatics Research and Innovation (CIRI), Digital Forensics and Cybercrime Lecturer - United States International University (USIU)

Carol Muchai | Information Security Consultant – Serianu Limited

Kevin Kimani | Information Security Consultant – Serianu Limited

Martin Mwangi | Information Security Consultant – Serianu Limited

Barbara Shiyayo | Data Analyst – Serianu Limited

Daniel Ndegwa | Data Analyst – Serianu Limited

Brencil Kaimba | Data Analyst – Serianu Limited

Faith Mueni | Data Analyst – Serianu Limited

Sylvia Shitanda | Data Analyst – Serianu Limited

Contributors

David Kabeberi - Managing Director, PKF Consulting

Joseph Mathenge - Chief Information Security Officer, Airtel Africa

Anne Kinyanjui - Partner, Iseme, Kamau and Maema Advocates

Wycliffe Momanyi - Chief Information Security Officer, KCB Bank Group

Edgar Mwandawiro - Head of Risk, Gulf African Bank

Evanson Ikua - Information Security Consultant

Collins Ng'eno - Head of ICT, Nairobi Hospital

George Okwach - Head of Audit, Crown Paints Limited

George Kisaka - Head of ICT Audit, Britam Insurance

Tyrus Kamau - Information Security Consultant and Chair of the AfricaHackOn

Design, layout and production: Tonn Kriation

For more information contact:

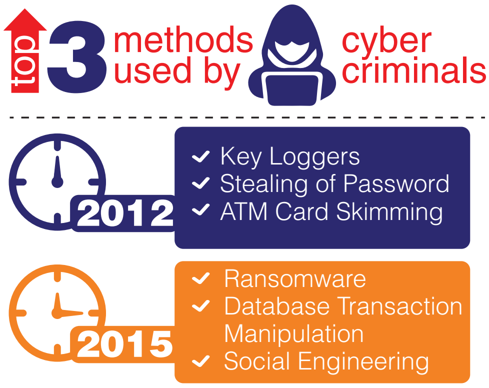
Serianu Limited, 14 Chalbi Drive, Lavington
P. O. Box 56966 - 00200 Nairobi, Kenya
Tel: +254 20 240 9294, **Cell:** +254 702 847 570
Email: info@serianu.com
Website: www.serianu.com

Three years of increased cybersecurity research, analytics and awareness..... and counting...

In 2012, we published the first edition of the Kenya Cyber Security Report. Three years later, the report's content and format has evolved but our primary objective remains the same: to provide local industries with a comprehensive view of the ever-changing cyber security threat landscape and enable them to make informed information risk management decisions. In 2012, cyber criminals were opportunistic in nature, but over time have become more skilled, focused and targeted in their attacks.

In 2012, many organisations were focused only on what security tools they should buy. This traditional approach focused on technology and point solutions that were not effective. The top 3 methods used by cyber criminals were key loggers, stealing of passwords and ATM skimming. In-comparison to 2015, the top 3 were ransomware, database transaction manipulation and social engineering.

Cyber criminals have advanced to such a degree that it is almost impossible to detect intrusions without the use of advanced continuous monitoring and detection methods. Their career is even becoming cheaper as their tools and attack mechanisms move to the cloud and are offered as a service.



In view of this changing environment, there is a need for organisations to spend more time understanding their operating environment (ICT infrastructure, People, Partners and Customers) and learning about cyber criminals who might target this environment.

Local cyber security professionals need to refer to a quote by Sun Tzu which emphasizes the concept of situational awareness. "It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles." Local organisations need to consistently look at the security, performance and availability of their critical network assets by enabling security

...our primary objective...
to provide local industries with a comprehensive view of the ever-changing cyber security threat landscape and enable them to make informed information risk management decisions...

Situational Awareness...

regular, repeatable development and communication of the organisation's knowledge of its people, ICT infrastructure, threats, incidents, and vulnerabilities.

professional in establishing cyber security situational awareness programs.

Security professionals need to focus on establishing cyber security situational awareness within their respective organisations. Situational awareness refers to the regular, repeatable development and communication of the organisation's knowledge of its people, ICT infrastructure, threats, incidents, and vulnerabilities. This capability focuses on understanding the cyber security posture of the organisation and driving effective decision making at all levels.

This year's report was based on feedback from our readers. As a result of these feedback we conducted a market survey to benchmark the current cyber security practices in Kenya.

> *"With evolving and dynamic cyber-attacks, timely sharing of cyber incidents and collaboration between Government and Industry will greatly improve Kenya's Cybersecurity preparedness"*
>
> **ICT PS**
> **Mr. Joseph Tiampati**

From the survey findings, we noted that respondents felt that most of the cyber security frameworks were global in nature and failed to address local situations where many small organisations have unique information risk requirements.

More than 50% of the participants also showed concern about the budgetary and resource constraints to effectively monitoring their ICT environment.

In response to this, we have shared a simplified cyber security framework that will enable local organisations to address major cyber security threats efficiently and pro-actively.

We are very excited about this years report and we hope it will provide you with new insights on the ever-changing cyber security landscape.

William Makatiani

About the Report

The Kenya Cyber Security Report 2015 was researched, analysed, compiled and published by the Serianu Cyber Threat Intelligence Team in partnership with PKF Consulting and the USIU's Centre for Informatics Research and Innovation (CIRI), at the School of Science and Technology.

Data Collection and Analysis

The data used to develop this report was obtained from different sources including; surveys and interviews with different stakeholders; several sensors deployed in Kenya and review of previous research reports.

The sensors are non-intrusive network monitoring devices that perform the function of monitoring an organisation's network for malware and cyber threat activities such as brute-force attacks against the organisation's servers. In an effort to enrich the data we are collecting, we have partnered with The Honeynet Project ™ and other global cyber intelligence partners to receive regular feeds on malicious activity within the country. Through such collaborative efforts we are able to anticipate, detect and identify new and emerging threats using our intelligent analysis-engine. The analysis-engine assists in identifying new patterns and trends in cyber threat sphere that are unique to Kenya.

Partnerships through the Serianu CyberThreat Command Centre (SC3) Initiative are warmly welcomed in an effort to improve the state of cyber security in Kenya and across Africa. This initiative is geared towards collaborative cyber security projects in academia, industry, commercial and government organisations.

For details on how to become a partner and how your organisation or institution can benefit from this initiative, email us at info@serianu.com.

TABLE OF CONTENTS

Executive Summary

The past year was a particularly tough period for local organisations with respect to cyber security. The number of threats and data breaches increased with clear evidence that home-grown cyber criminals are becoming more skilled and targeted. This means that local organisations will continue to lose as they scramble to change their defensive stance.

According to the latest internet usage report from Communications Authority of Kenya, there were an estimated 26.1 million internet users in Kenya as of December 2014. This is equivalent to 64 percent of the country's total population with access to the internet and over 70% being below 25 yrs.

Compare this to the number of information technology and security risk professionals in the Kenyan market. According to ISACA Kenya, there a total 1,000 certified ICT risk professionals in the market. Which means there is approximately 1 security professionals for every 200,000 internet users. This is a worrying ratio that needs to change if we are going to successfully secure the cyber space in Kenya.

By the year 2017, it is estimated mobile broadband subscriptions will approach 80% of the country's total population. By the year 2020, the number of networked devices (the "internet of things") will outnumber people by six to one, transforming current conceptions of the internet. In the hyper-connected world of tomorrow, it will become hard to imagine a "non-computer crime," and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity.

At Serianu, we have witnessed the ever-evolving technology landscape and believe the next twelve months will only give cyber criminals more opportunities to infiltrate the networks that store business and consumer data. Considering the vulnerabilities and attacks we have seen in the past year, it is clear our exposure is growing. The key to protecting data is to develop realistic and prioritized strategies around situational awareness and pro-actively implement them.

2016 PRIORITIES

Our Priorities in 2016

1 Cyber security monitoring and human based log analysis is no longer an option but a NECESSITY

The type of attacks local organisations experienced in the past year clearly confirms that traditional, signature-based security measures are simply inadequate when it comes to stopping today’s cyber criminals. You can no longer rely on automated solutions to protect your data. Cyber criminals are very proficient at bypassing multiple automated defenses and have many social engineering tricks in their arsenal to leverage people’s habits to their advantage. Fortunately, most attacks on your network leave behind indicators that signal a problem. Organisations need to put in cyber security monitoring processes to identify these behaviours, and alert relevant personnel to resolve the issues.

2 There is a need for MANDATORY Employee Security Awareness and Training

No matter how you look at it, people continue to pose the greatest cyber security risk to organisations. People are known to be the weakest link in the security chain. The latest security technology may protect core systems, but it cannot protect against employees giving away information on social networks or using their own, less secure, mobile devices for business purposes. Organisations need to invest in security awareness and training - that covers cyber security practices in the office, such as protecting passwords, how to deal with phishing and other social engineering attacks and also how to enhance privacy settings on social media sites.

3 Every organisation must develop Localized cyber intelligence and research

In our analysis of cyber intelligence, we have noted an increase in the number of Africa-based cyber criminals, especially from Nigeria, Rwanda and Kenya. This is a clear indication that Africa is increasingly becoming a source of cyber criminals and tools. Most recently, we uncovered a cyber criminal ring that was harvesting Facebook account information from Kenyan users and some financial institutions and leveraging this information for profit. Localized Cyber intelligence and research is critical in understanding the type of attacks that your peers are facing in the region. While many technology vendors will provide you with cyber intelligence - our experience has been that this intelligence is global in nature and does not put into account any local intelligence. To be fully secure you need to develop local cyber intelligence capabilities that will enhance the visibility of the threats facing your organisation.

4 Third Parties require mandatory and regular VETTING

Outsourcing is not just a growing trend but the new reality of today's rapidly evolving global economy, which raises a new set of risk management concerns for companies in every industry. Organisations are increasingly relying on third parties to provide and enable more critical services across the region. In fact there are cases where some organisations have outsourced over 70 percent of their operations and they rely on third parties to provide mission critical services to their customers and counterparties. Cyber criminals are frequently able to exploit vulnerabilities in the third party's networks to get to the target company's assets. Local organisations need to hold third-party entities to the same Cybersecurity standards and protocols that the organisation itself follows internally. Otherwise, you unnecessarily put your company's reputation and financial health at risk.

5 Organisation should EVALUATE the need for Managed Security services

Many organisations are finding out that they are ill-equipped to handle the complex and multiple cyber threats posed to them. As a result many organisations are looking at managed security service providers to ensure that their IT infrastructures are secured against attacks and potential security breaches. In the past year, 10 different organisations issued RFPs (Request for Proposals) for managed security. Many organisations are looking at managed security services as the most cost effective and efficient way to maintain the competency of the organisations without restraining the growth of an organisation against its competitors. At Serianu we believe Managed Security Services are necessary to manage the growing computing complexities and increasing threats and cybercrimes, without interrupting organisations' business operations. Local organisations need to identify key areas that can be outsourced and seek out vendors to support their internal security strategies.

Bonus Priority:

Vulnerability Assessment and Penetration Testing is not enough

Organisations need to implement holistic programs that incorporate patch management, vulnerability management, continuous monitoring, and Incident Response and remediation strategies to effectively mitigate any vulnerability in their environment .

Cyber Security Perspective from the Professional Services Sector

David Kabeberi | *Managing Director, PKF Consulting*

With the recent uptake of fiber connectivity in Kenya, broadband and internet access has become readily available to the everyday citizen. General Cyber Security threats (like malware attacks, social engineering scams and financial fraud, etc.) have increased. Based on our extensive experience in the local market, a large majority of companies often adopt the wrong attitude of 'this won't happen to me'' (referring to IT security risk). These companies are more focused on market share growth rather than taking proactive measures to mitigate security risks. However, this is a dangerous viewpoint to take. No company – no matter its size - is safe from cyber threats.

SMEs can be victims to a wide range of cyber security threats, including phishing, malware, online banking fraud, the threat of the Bring Your Own Device (BYOD), data corruption and data loss. It is thus essential that SMEs put the right Security policies and practices in place from the start. This will not only help curb cybercrime, but will also give companies peace of mind that their data is protected against attack.

Today cyber criminals are evolving and innovating new ways to target companies. They are targeting perceived vulnerable companies not directly but through their weakest links, their employees. In fact, over the years, threats focused on businesses have shifted from vulnerabilities in corporate software and moved to target the user of these systems. The logic being, hacking the person is easier than hacking these reinforced systems.

Often users lack the adequate training and awareness to be able to defend themselves against these social engineering attacks. Once attacked, users often unwittingly share confidential information that compromises them and in some instances even the companies they represent. According to Kaspersky Security Network (KSN) statistics for April-June 2015 overall 14.7% of KSN participants in Kenya faced web-borne threats, and 39.7% faced local threats (Social Engineering, USB, flash drives, local networks).

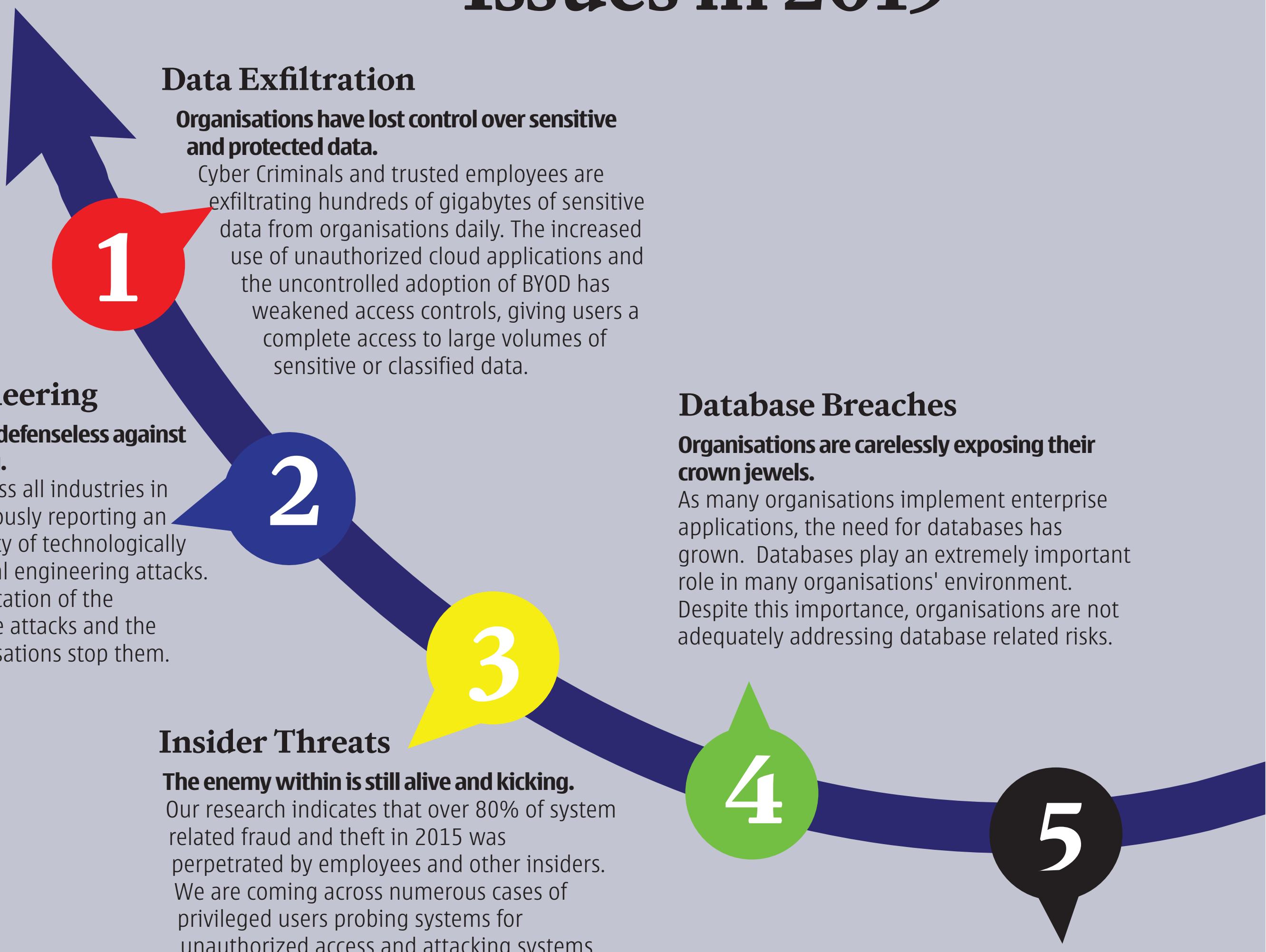
While security can be resource intensive in the initial stages, the return on investment in safeguarding confidential information and IP will more than make up for this. It is important to realize that having the right security processes in place will help a company in the long-term and as a result can save a company losses both financial and reputational. The caveat lies in avoiding cumbersome and expensive "corporate" security, or "consumer" security solutions not designed for your business needs and focusing on simple, reliable, practical solutions that are easy to use and offer good value.

We believe security awareness and gaining visibility of your security posture is key and business owners should continuously keep informed on emerging cyber security risks and steps that should be taken to avoid them, and share this knowledge with their peers.

Focusing on the basics should therefore be a key message from industry and government bodies to local business and more support should be provided to help them take tangible steps in this area.

PKF Consulting is doing its part by playing an active role in the wider policy debate about how best to support businesses to improve cyber security practices. Through expert risk assessment, advisory and support provision for companies on cyber security issues, raising awareness of cyber risks and providing practical guidance on the steps that businesses can take.

Top Cyber Security Issues in 2015



Data Exfiltration

Organisations have lost control over sensitive and protected data.

Cyber Criminals and trusted employees are exfiltrating hundreds of gigabytes of sensitive data from organisations daily. The increased use of unauthorized cloud applications and the uncontrolled adoption of BYOD has weakened access controls, giving users a complete access to large volumes of sensitive or classified data.

Social Engineering

Organisations are defenseless against social engineering.

Organisations across all industries in Kenya are continuously reporting an increase in a variety of technologically sophisticated social engineering attacks. This is a clear indication of the popularity of these attacks and the inability of organisations stop them.

Insider Threats

The enemy within is still alive and kicking.

Our research indicates that over 80% of system related fraud and theft in 2015 was perpetrated by employees and other insiders. We are coming across numerous cases of privileged users probing systems for unauthorized access and attacking systems for a variety of reasons including disgruntlement, revenge, and financial gain.

Database Breaches

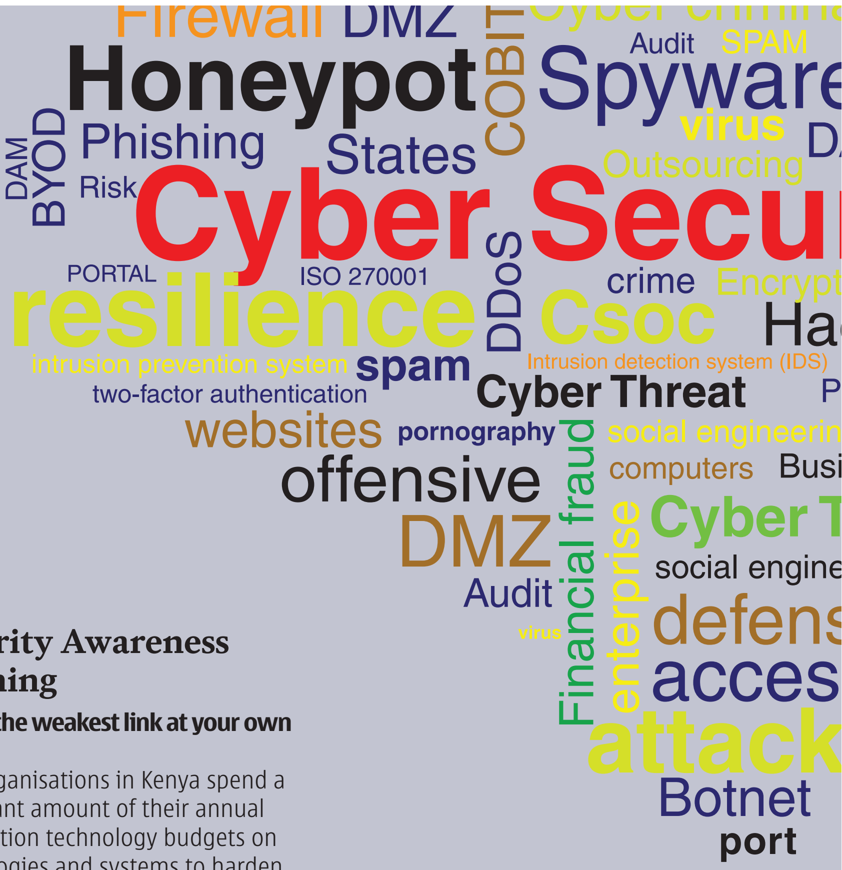
Organisations are carelessly exposing their crown jewels.

As many organisations implement enterprise applications, the need for databases has grown. Databases play an extremely important role in many organisations' environment. Despite this importance, organisations are not adequately addressing database related risks.

Poor Identity and Access Management

Uncontrolled identities and access control are exposing organisations.

Identity and access management processes and technologies are not well adopted in most local organisations. Leading to unauthorised and inappropriate access to highly sensitive information.



6

Continuous Monitoring and Response

Almost all organisations are not prepared for cyber threats.

In our survey, we noted that majority of the organisations are ill prepared to monitor and respond to cyber attacks. 90% of Kenyan organisations have no real-time insight on cyber risks, lacking the agility, budget and skills to combat rising cybercrime. Majority of these organisations are unable to detect cyber attacks using the existing systems and processes.

7

Vulnerability and Patch Management

The achilles heel of organisations cybersecurity efforts.

Our study reveals that majority of Kenyan organisations do not perform regular vulnerability scans on their network thus are unable to tell their current security posture.

8

Security Awareness Training

Ignore the weakest link at your own risk.

Most organisations in Kenya spend a significant amount of their annual information technology budgets on technologies and systems to harden their infrastructure ignoring the untrained, uninformed or unmonitored users. Without training, most users in Kenya don't have the skills and knowledge they need to adequately protect the organisations' infrastructure and informaiton from cyber attacks.

9

Inadequate Budgets and Management Support

Put your money where your risks are.

A great percentage of organisations in Kenya are operating with little or no budget or management support. In most of these organisations executives are not willing to dedicate funds towards the purchase or engagement of cyber security solutions or services. Often these organisations are waiting for a breach before they can react or act.

10

Emerging Technologies and ERP Automation

Automation minus controls equals to risks.

Many organisations in Kenya are implementing Enterprise Resource Planning (ERP) that automate and integrate a company's core business and help them focus on effectiveness and simplified success. ERP systems are helping increase productivity, efficiency and accuracy but at the same time they are introducing new risks to organisations.

Cyber Security Perspective from the Academic Sector

Paula Musuva Kigen | *Research Associate Director, Centre for Informatics Research and Innovation (CIRI), Digital Forensics and Cybercrime Lecturer, United States International University (USIU)*

This is yet another year of great insights from the Serianu Team. This year the Kenya Cyber Security Report gives us local intelligence into the top Cyber Security challenges organisations are facing in Kenya.

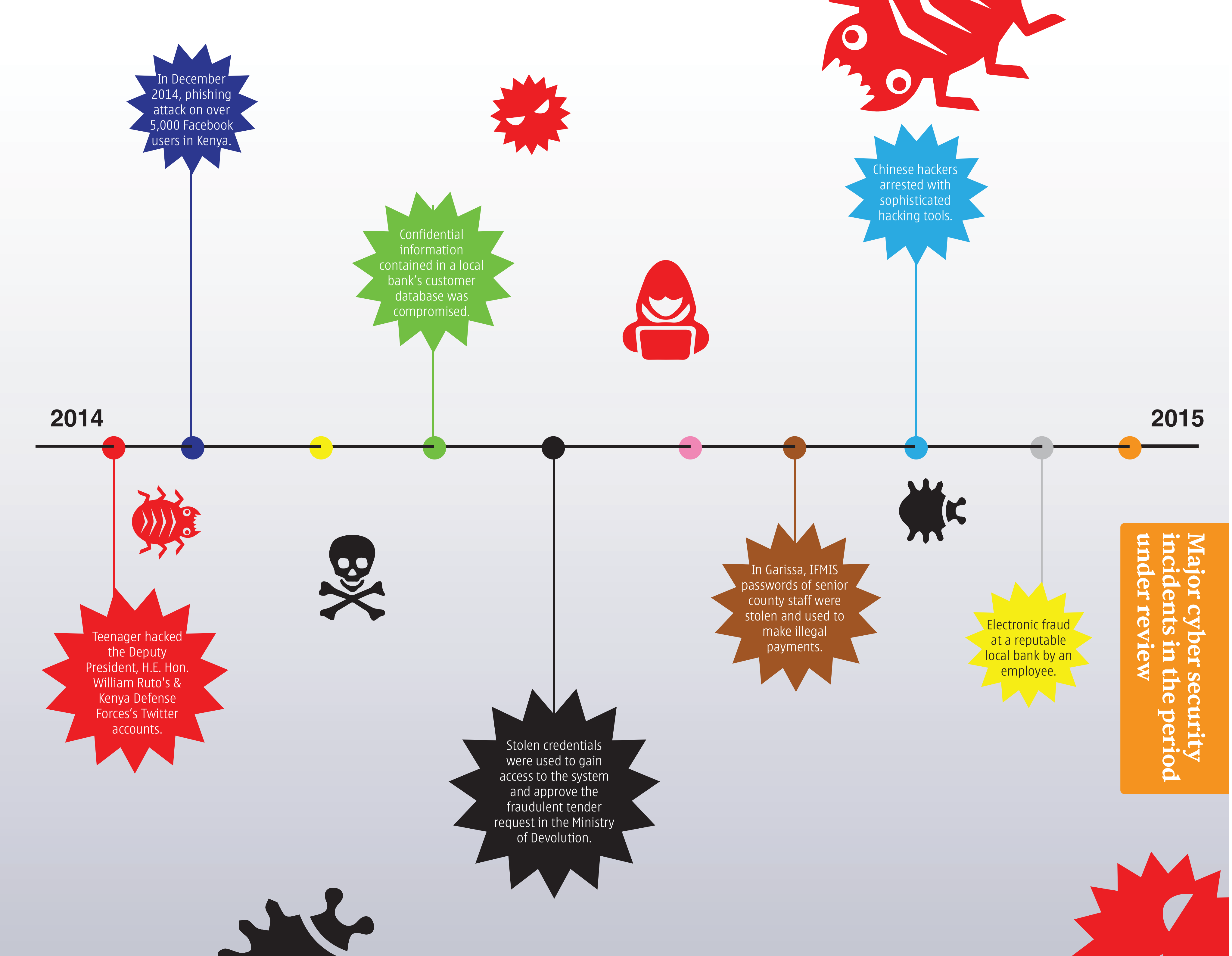
I have been fortunate to collaborate as an academia partner in designing the data collection instruments, analysing data and documenting it in this report. This is an important role that academia partners can play in the cyber security space. Research is our strength based on skill, time and human resource. Academic institutions have students who can be co-opted into research projects. They can offer the manpower for data collection and in the case of post-graduate programs (masters and PhD) they can devote time in research to solve specific cyber security problems. It is true that many organisations would be weary of contracting students to undertake cyber security research but there are areas of low risk that could be considered. Examples of low risk cyber security problems that can be addressed through student research could relate to security testing of business applications to identify vulnerabilities, analysis of data from security information and event management (SIEM) systems to identify attack patterns, design of customized algorithms that indicate compromise, customizing tools to capture security events for example based on honeypot and honeynet technologies.

Another key contribution that academia partners can bring is in conducting Cyber Security Education, Training and Awareness – commonly referred to as SETA. The common sense knowledge in cyber security is lacking among many employees and in the general public. Training seminars and workshops can be offered by university professors in organisations at reasonable and competitive costs. Training curricula and materials can be developed in collaboration with the information security departments in the organisation in order to capture the pressing needs of the organisation.

Universities are now also offering undergraduate and post-graduate degree programs with specializations in Information Security. In addition, some universities are now partnering with professional bodies and key industry players such as ISACA, Cisco, IBM, Microsoft, Ec-Council to offer industry recognized certifications to their student body. This is to help bridge the skills gap by providing top quality graduates in cyber security. Notable initiatives that kicked off in 2014 include the IBM Middle East and Africa (MEA) University program, which is part of the IBM Academic Initiative. There are many disciplines covered in the IBM MEA University program and Cyber Security and Information Assurance is one of them. Another by ISACA is the Cybersecurity Nexus which was launched in 2014. The entry point for students and recent graduates is the Cybersecurity Fundamentals Certificate which gives employers confidence in the Cybersecurity knowledge the graduate has.

It is our hope as academic partners that we can form synergies with industry in the areas of research, training and skills development. We hope to have active Academic Centers of Excellence for Cyber Security in the near future. Such initiatives will go a long way in securing our region's cyber space.

Major cyber security incidents in the period under review



Teenager hacked the Deputy President, H.E. Hon. William Ruto's & Kenya Defense Forces's Twitter accounts.

In December 2014, phishing attack on over 5,000 Facebook users in Kenya.

Confidential information contained in a local bank's customer database was compromised.

Stolen credentials were used to gain access to the system and approve the fraudulent tender request in the Ministry of Devolution.

In Garissa, IFMIS passwords of senior county staff were stolen and used to make illegal payments.

Chinese hackers arrested with sophisticated hacking tools.

Electronic fraud at a reputable local bank by an employee.

Cyber Security Perspective from the Cyber Security Sector

Tyrus Kamau | *Information Security Consultant and Chair of the AfricaHackOn*

It has indeed been an eventful year for cyber security globally. Right from the Sony Hack, Hacking Team's leak, Android's Operating Systems' numerous vulnerabilities, General Motors' Jeep hack, the list goes on.

Locally, we saw a sharp rise in financial fraud within banks through mobile money, system tampering and mobile network exploitation. All these have received wide coverage from the main stream media lending credence to the fact that situational awareness around the subject is gaining wide spread attention compared to previous years.

On the ground, it's a different ball game. We are still seeing very few capable information security practitioners, insufficient reporting of cyber security incidences and a hands-off approach by the respective Government bodies. Granted, there have been institutions set up like the KE-CIRT housed at the Communications Authority (CA) which by now should be providing guidance and leadership in all matters cyber security. In addition, we are seeing a very fast proliferation of technologies such as NFC which, as show cased in the recently concluded AfricaHackOn conference, have inherent vulnerabilities which banks & merchants need to address sooner than later.

The issue around capacity building is one that will propel the country into a more proactive approach towards the subject, whereby entrants to the space will push the envelope in terms of Research & Development, curriculum realignment, legislation and compliance. This has been AfricaHackOn's mission through university & college bootcamps, training programs and industrial placements for those who go through our course.

In conclusion, there is need for a local professional body to enshrine some core philosophies which are unique to our ecosystem as opposed to borrowing heavily from international best practices.

Cyber Security Risk Ranking by Sector

Government

1

The public sector (government and related parastatals) are adopting technology and automating processes. This includes implementation of IFMIS system, E-procurement, ITax and IPRS. These systems hold huge volumes of 'mwananchi' confidential information and capabilities of approving payments and funds transfer. The continued automation, centralization of systems, limited investment in information security, lack of defined processes and previous cases of fraud influenced our decision to rank the public sector as the sector facing the highest cyber security risk in Kenya.

Banking

2

The banking sector comes in at a close second as a high value target to cyber criminals because they have money and due to their increasing reliance on technology and third parties to perform and enhance their management and transfer of money. Mobile and online banking channels carry with them inherent risks as they expose previously closed processes to the internet and the public.

Financial Services & Mobile Money

3

Kenya is at the global forefront of mobile money services as an alternative to traditional banking. These innovations are seen as new payment channels and online services that facilitate easier access to money. These new channels have opened new alternative targets for cyber criminals. Instead of targeting banks - cyber criminals are now targeting financial services (payment systems, mobile money) service providers to access bank systems.

Manufacturing

4

For many years, manufacturing organisations in Kenya have relied on simple accounting or manual controls to mitigate fraud. This has changed over the past 5 years as these firms have implemented ERP systems that automate the entire manufacturing lifecycle. Unfortunately, majority of these organisations have not implemented the requisite controls to ensure they can detect and prevent system fraud. The lack of controls has led to a huge and sudden increase in system fraud targeting key financial processes in the manufacturing sector.

Sacco's

5

Historically, Sacco's have relied heavily on manual or basic transactional systems to run their back-end operations. As the sector has grown and transactional volumes increased, Saccos are now automating their back-end operations. Many Sacco's are now automating their back-end operations. Unlike banks, Sacco's lack skilled security personnel and anti-fraud systems. This has lead them in becoming greener targets and a higher chance of success for cyber criminals.

Telecommunications

6

Telecommunication service providers in Kenya are a prime target for cyber criminals. As the country's reliance on technology continues to growth with all organisations (banks, government etc) relying on internet connectivity from telcos. Cyber criminals are targeting these organisations because of three main reasons: the control and operate critical infrastructure in the country; they store large amount of sensitive customer information, and they facilitate mobile money services in the country.

Insurance

7

Like other sectors, the insurance sector in Kenya struggling with process automation and implementation of new technologies like cloud, mobile and big data. Most of the risk in the sector is attributed to malicious insiders who access systems to make unauthorized changes to key financial/customer systems, transfer money illegally and steal customer/brokerage files. As the sector continues to introduce new internet related channels the level of cyber risk is also growing.

Retail

8

Historically, Criminal activity targeting Kenyan retailers was mainly manual and involved shoplifting and other physical theft of merchandise. The recent automation and innovation had led to new cases of fraud involving systems. This includes credit card fraud targeting retail customers, malicious manipulation of data in retail/loyalty systems, and unauthorized payments. There is no doubt these level of sophistication will continue to grow as the industry automates and innovates.

Hospitality

9

Due to Kenya's positioning as a top tourism and business destination. The country attracts hundreds of thousands of global visitors every year. To ensure they can cater for the global visitor, most of the organisations have invested in the use of technology to efficiently collect, process and store huge amounts of customer and payment data. Most of these organisations have not invested in information security practices which makes it one of the most vulnerable sectors in the country.

Professional Services

10

Majority of consulting and professional services firms (strategy, marketing, law and audit firms) in Kenya have not implemented cyber security measures similar to the mitigation strategies put in place by the corporate clients they work with. Consider that most of these firms hold lots of sensitive corporate information. Cyber criminals are targeting these firms to get access to marketing plans, financial documents, litigation documents and strategy documents. There are cases where internal employees are leaking information to external parties. As long as cyber criminals think they can easily get access to a corporate clients critical information from a professional services firm. They will target these organisations instead of going directly to the corporate clients network.

Cyber Security Perspective from the Telecommunications Sector

Joseph Mathenge | *Chief Information Security Officer, Airtel Africa*

Bake in and not sprinkle on security

Historically, telecommunications have traversed voice services over a switched-circuit-style network. In the recent years however, the growth of IP packet based network, also known as Next Generation Network, has seen the use of multiple broadband transport technologies and has fueled growth of mobile data services through smart phones.

As Africa closes in on 1 billion mobile subscriptions, a recent report by global technology consulting firm, International Data Corporation (IDC), predicts smartphone shipments will top 155 million units by the end of 2015 in the Middle East and Africa having increased by 66% during the first quarter of 2015.

While the migration to this new platform allows consumers greater value in voice and data communications, it brings with it a whole host of security challenges. Issues that have bereft IP based network, ranging from unauthorized network intrusion, spread of malware to the destructive effect of Denial of Services (DOS) attacks.

So have we learned from the experiences of challenges of an IP connected world? As we reinvent the telecommunication industry and weave technology deeper into our lives how much are we exposing our inherent vulnerabilities?

As security practitioners our goal is defined; protect the information asset while in use, transit or at rest. We must deploy the same fundamentals with the understanding and pragmatic view of this environment so as to effectively protect it.

I want to highlight 3 key principals that can be used.

1. Know your assets – You simply cannot protect what you don’t know about. In a Telco environment,where there are nodes of both IP and non-IP based network this can be a daunting task. More so the environment gets extended when the infrastructure provides connectivity to critical services providers such as healthcare, financial or lately energy distributors.

2. Configure and maintain them securely. One of the most common causes of systems intrusion is poorly configured or unpatched system. Ponemon Institute conducted a survey on Data Security Breaches that revealed the number one leading cause of data security breaches resulted from non-malicious employee error (39%). These breaches were typically the consequence of complacency or negligence from lax or insufficient access controls to sensitive or confidential data. This is perhaps the most difficult activity and one that too many organisations in all industries do poorly.

3. Detect quickly and respond effectively to systems security event. It’s been said that the only safe communication device is one that you buy and bury. If you think about it, that beats the purpose in that, we buy these as tools to facilitate communication and commerce. Keeping that in mind, it simply means that sooner or later, even the most securely maintained environment would be victim of a cyber security event. Accordingly, we must prepare by putting in place ability to monitor all activity, detect anomalies, define if these are malicious and respond quickly and effectively to minimize the effect.

In conclusion, we must design and implement systems that cater for our need to effectively communicate while accounting for known and unknown security threats to our information assets.

Top ICT Trends Influencing Cybersecurity in Kenya

Cloud Based Solutions

Many organisations in Kenya are steadily embracing cloud computing solution for different business and technological benefits, further driving their migration to cloud computing. Majority of these organisations have adopted cloud application services like google (Google Apps), Oracle Cloud, Microsoft (Microsoft 365).

ERP Automation

Many organisations are moving away from siloed systems and adopting enterprise wide systems (Enterprise Resource Planning (ERP)) that automate and integrate the organisations core business processes. These organisations need these systems (ERP) to be competitive.

Outsourcing and Managed Services

Most Kenyan organisations don't possess all the skills and expertise needed to complete every project in-house. These organisations are turning to third-party providers for a variety of essential business needs especially for IT and business process management.

Mobile & Internet

Almost all major retail service providers have rolled out a range of mobile or internet enabled services . These services provide a convenient platform for customers and also reduce the cost of physically servicing their clients

Commercialization of Hacking

The hacking community has moved into the commercial space by offering their tools and skills as services that can be paid for through untraceable virtual currencies such as Bitcoin.

Industry Regulation

Regulation especially from the CBK is forcing many regulated organisations to implement security controls. Currently , CBK carries regulatory compliance checks which require the regulated organisations especially banks to implement relevant controls to mitigate risks.

Bring Your Own Device (BYOD)

Studies have shown that this trend increases productivity by allowing an employee to bring a device they find comfortable and easy to navigate. In addition, the Company saves on cost since they have no responsibility over furnishing the employee with a device. However, it also introduces new risks especially when employees are allowed to access privileged company information and applications on these devices.

Teleworking

Organisations in Kenya are slowly but surely embracing teleworking by Employees by allowing employees to work from home or away from the office. The remote access to enterprise infrastructure enables employees to work within the confines of their homes thus saving time, money and gaining an optimum work-life balance.

Internet of Things

The Internet of Things (IoT) refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.

The growth of IoT opens up new attack vectors both in terms of type of data generated and the variety of devices connected to the Internet, giving attackers an easy way to penetrate the networked data.

Near Field Communication

A number of companies in Kenya have introduced NFC technology. These companies include Card Planet, Abiria card, Gigwapi, Buymore, BebaPay (replaced with Equity prepaid MasterCard) and my1963 cards. Shopping outlets are also using NFC cards to offer loyalty programs to their customers enabling them redeem points based on their expenditure. NFC is inherently at risk of eavesdropping and interception attacks.

Cyber Insurance

Two insurance companies in Kenya are now offering Cyber insurance covers for liabilities related to cyber-attacks. These companies also cover processes related to investigations, remediation, call management, credit checking for data subjects, legal costs, court attendance and regulatory fines during the period. We expect this trend to continue as many other companies create similar products.

2015 Kenya Cyber Security Survey

The purpose of the 2015 Kenya Cyber Security Survey was to explore and identify the needs of Kenyan businesses and to find out what they see as the potential cyber security threats both now and in the future. As perceived threats may be different from real threats, it is important to try to correlate local organisations' experiences of cybercrime with the situation as reflected in current reports and analyses.

Key Survey Findings

About the Report

This survey report was prepared based on data collected from a survey of 275 organisations in Kenya. This includes 175 technical respondents (predominantly chief information officers, chief information security officers, IT managers and IT directors) and 100 non-technical respondents (procurement managers, senior executives, board members, finance professionals and office managers). The survey measures the challenges facing Kenyan organisations and the security awareness and expectations of their employees.

Summary of Findings

Most respondents believe criminals are increasingly targeting their organisations, however, many report that their organisations do not have enough staff and security expertise dedicated to information security.

The majority of respondents say their organisations are increasingly becoming concerned and have partially implemented proper security precautions, technology and training. The security measures most often reported as being implemented by IT practitioners are perimeter systems like firewalls and anti-viruses.

In Manufacturing and Government sectors, respondents say there is either no or some level of cyber security controls. Respondents in these industries report that firewalls are the main security measures in place to prevent targeted attacks. This is followed by anti-virus technology.

Cybercrime was seen by survey respondents as a problem rooted primarily in economic interests and in technology.

One of the findings of the survey was that most respondents consider "better education of users of the Internet" as the single most important topic that should be researched in order to make the Internet a safer place (35% of respondents).

"Improve our understanding of society and our cyber community" scored the next highest in the very important category (22% viewed this as very important), while "better laws and regulations" were viewed as very important by only 6%. Most respondents, however, rated "Better metrics and statistics on cybercrime" as their 3rd choice after selecting their top choice of topic for more research.

Indeed, the above responses seem to correlate with the response to another question, concerning training within their organisation: 64% of respondents were not trained in cybersecurity issues at all or only if there was a problem (note: we included "don't know" responses in this category as well). Even though many respondents considered cybercrime to be a concern and many had been victims either personally or as part of their organisation (as many as 78%) most respondents declared that the main consequence of the cybercrime action was inconvenience (50% of respondents).

Another very visible problem is the relatively low reporting rate of cybercrime to the Police (73% of cybercrime cases not reported) and/or national CERTs (74% of cybercrime cases not reported). This is followed up by a low successful prosecution rate: only about 10% of the cases were successfully prosecuted.

Information sharing in general was found to be a problem (only 27% respondents said they or their organisation shared information on cyber-attacks) - an issue that also hinders effective measurement of cybercrime.

Overall, however, the initial findings appear to confirm that there is a tangible need for better definitions, metrics and statistics for cybercrime together with more training.

Survey Findings and Risk Groupings

1 **20% respondents LACK sufficient cyber security budgets.**

20% LACK cyber security budgets while 28% Allocate **LESS** than Kshs.100,000

2 **Although 61% allow BYOD an alarming 59% LACK policies and procedures to manage them.**

61% **Allow** BYOD

59% **Lack** policies or procedures

3 **21% of the organisations are NOT concerned about cyber crime.**

79% Concerned about cybercrime in their organisations While 21% **NOT** at all concerned

4 **87% agree cybercrime is a real issue in the organisation**

87% Agree cybercrime is a real issue

13% Not an issue

Cyber Security Perspective from the Financial Services Sector

Wycliffe Momanyi | *Chief Information Security Officer, KCB Bank Group*

Financial transactions are increasingly administered in real time with minimal human involvement. This is being driven by customer demand for faster, more efficient, easier and more secure means of carrying out their transactions. As a result of the ever increasing roll out of technologically driven products, the financial sector is facing ever-escalating threats from cyber criminals.

While vulnerabilities in software and network continue to be the target of cyber attackers and defending these resources remain the focus of every organisation, the weakest link continues to be the user/ people. Data breach arising from phishing attacks and social engineering continues to be on the rise. Banks have made efforts towards educating their clients including providing information on their Internet banking portal though in the face of a targeted attack, these efforts are proving to be inadequate. Social media provides the platform required for an attacker to mine information on an individual. This information is then used to make the user believe that he is communicating with a legitimate source. With easier access to social media and the tendency to share personal information, the number of users that are exposed to such attacks will continue to increase.

Conversely, Mobile banking has taken center stage with most financial institutions adopting mobile related services and mobile devices getting more powerful every year. Smart phones available today are capable of carrying out all the functionalities generally done on a PC. While there are efforts made to ensure that a PC is kept secure, a smart phone that does the same functionality does not receive similar attention. Mobile devices and mobile service offering have become an attractive and easy target for cyber criminals owing to the lack of knowledge of users on the potential hazards as a result of for instance the download of a malicious software.

In 2014, J.P. Morgan Chase & Co, the largest U.S. bank by assets conceded that unknown attackers stole about 76 million customers' contact information - including names, email addresses, phone numbers and addresses. These breaches happened to JP Morgan Chase which spends billions of dollars to fund IT budgets and employ large teams of security analysts pointing to the sophistication of these cyber attacks. It is also reported that it took over a month for JP Morgan to detect that they had been hacked, for Kenyan banks it's a major challenge and one can only guess the extent of the problem.

Insider fraud is one of the major contributors to cybercrime and a headache to all Information Risk & Security practitioners. The employees are assigned privileged access to systems and thus it is easier for an insider to carry out a cyber-attack as he is already aware of all the security devices and procedures in place. An attack by an insider is often more difficult to identify and recover from, vendors pose the same risk with a possibility of more devastating attacks.

From experience it is evident that even the best preventive solution is bound to have vulnerabilities that attackers can exploit, therefore becomes now whether but when an attack will take place and what measures have we set in place to respond to these attacks.

To address the unintended failures, an institution is expected to take several steps such as adoption of Board-approved IT governance policies, establishing data centres, third party contracts, robust service level agreements, IS audit etc. As far as the risk of unintended failure is concerned, the IT management policy framework that has evolved over a period of time along with corporate governance has addressed the risk factors to a large extent. All these have come at a huge cost, but a definite resilience has been achieved. However the intended intrusions to disrupt business, misuse the information available at the institutional level.

To implement the kind of customer protection as discussed above, it is important that the insurance sector also responds. Even in the US, companies lament that insurance covers do not give adequate financial indemnity to losses arising out of cyber-attacks. An insurance cover against cybercrime or cyber failure would mitigate the risk to a large extent. There has been effort to come up with such products but the same needs to be refined to provide comfort to banks.

5 **99% Believe cybercrime is here to stay but is solvable.**

99% Cybercrime is **SOLVABLE**

while

1% Cybercrime is **NOT** an issue

6 **64% of the respondents have not implemented REGULAR Employee awareness and training.**

64% Never or only if there is an issue

while

ONLY 36% Have regular employee awareness and training

7 **Upto 73% of cyber crime victims do NOT report these crimes while 13% did not know HOW to report these incidents.**

73% Do **NOT** report cybercrime

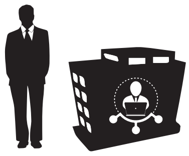
while

27% Did **NOT** know **HOW** to report these incidents

8 **50% are neither aware of WHAT a CERT is nor HOW to contact them in case of an incident.**

50% Dont know WHAT a CERT is

9 Up to 57% rely on an in-house System Administrator to handle security functions.



upto **57%**

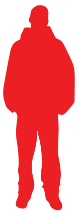
RELY on In-house System Administrator to handle security functions

while

13%

DONT know who handle security functions

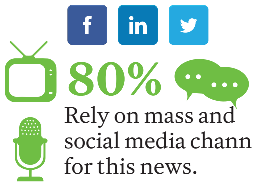
10 20% do not review current cyber security news.



20%

Do **NOT** review

while



80%

Rely on mass and social media channels for this news.

11 Only 27% of the organisations share information to improve security awareness.

27%

SHARE information to improve security awarenesss

12 Less than 5% of local organisations have purchased database security monitoring tools.

less than **5%**

NOT purchased database security monitoring tools

13 Better education of users of the internet at 35% as the most important topic to be researched in order to fight cybercrime.

35%

Better education of users of the internet

14 19% are more concerned about their payment systems being attacked by cyber criminals while 3% are concerned of their mobile devices.

19%

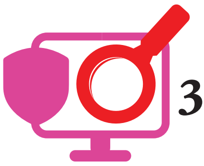
Concerned about their payment systems

while

3%

Concerned only for their mobile devices

15 35% do not utilize security testing tools while only 24% use vulnerability scanning and penetration testing tools.



35%

Do **NOT** utilize security testing tools

while

24%

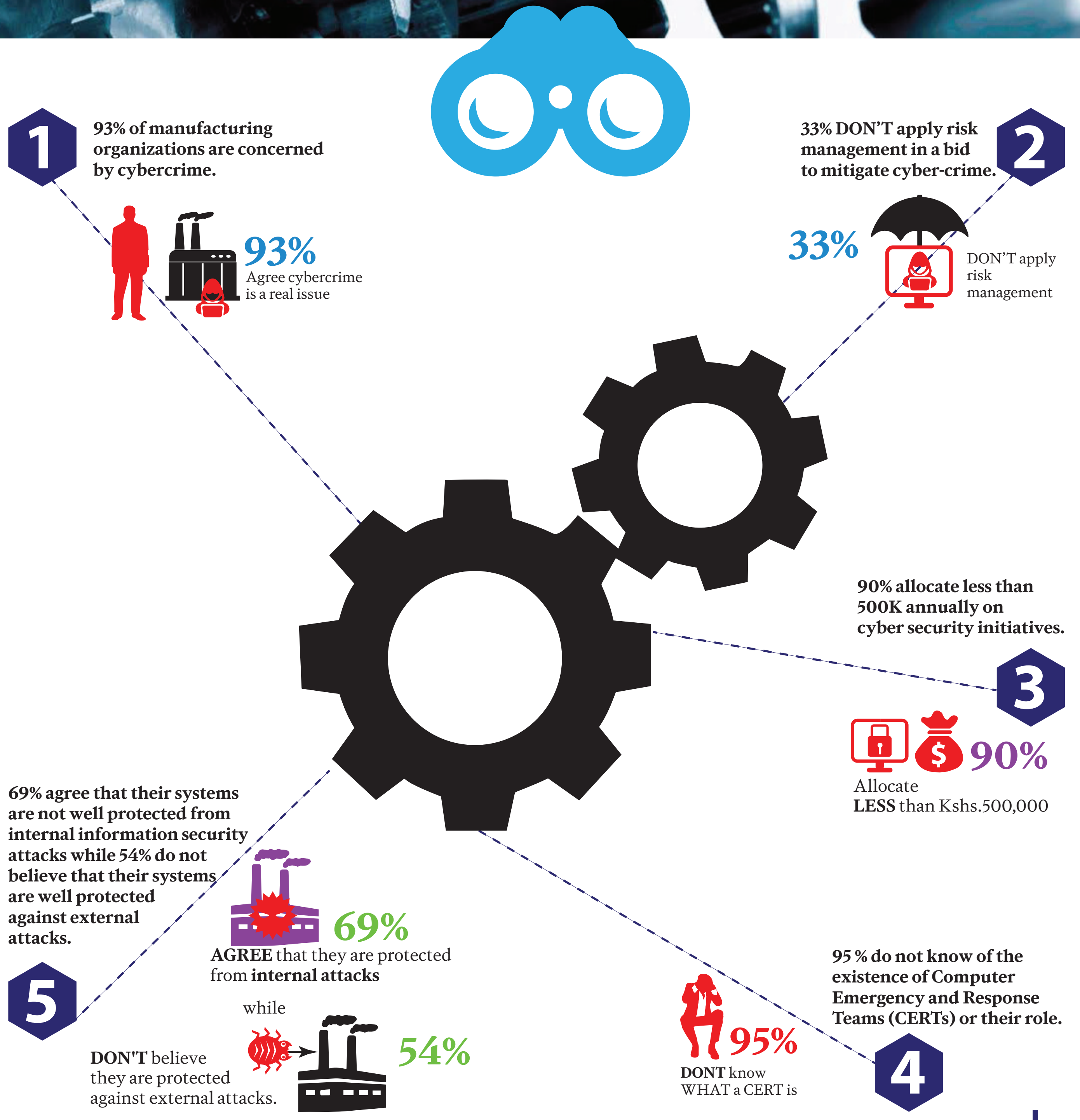
Use vulnerability scanning and penetration testing tools

16 33% know the description of cybercrime.

ONLY **33%**

KNOW what is cybercrime

Manufacturing Sector Analysis



1 93% of manufacturing organizations are concerned by cybercrime.

93% Agree cybercrime is a real issue

2 33% DON'T apply risk management in a bid to mitigate cyber-crime.

33% DON'T apply risk management

3 90% allocate less than 500K annually on cyber security initiatives.

90% Allocate **LESS** than Kshs.500,000

4 95 % do not know of the existence of Computer Emergency and Response Teams (CERTs) or their role.

95% **DONT** know WHAT a CERT is

5 69% agree that their systems are not well protected from internal information security attacks while 54% do not believe that their systems are well protected against external attacks.

69% **AGREE** that they are protected from **internal attacks**

while

54% **DON'T** believe they are protected against external attacks.

Cyber Security Perspective from the Cyber Security Sector

Evanson Ikua | *Information Security Consultant*

Nothing fascinates me more than technology. While going through my old trash when moving house last year, I came across a few things that I had forgotten still existed. One of them was my High School ID card and the second was my Postbank book. The latter reminded me of my college days when I would bank my boom and gradually withdraw the same as needed. Every time I needed to deposit or withdraw some money, I had to carry along my savings book to the Bank and the teller would record my transactions on that book and also record my balance. Losing the book meant a tedious process for the bank to go into the ledgers to manually reconcile my records.

That was in the early nineties. It still amazes me that we could still arrange and keep dates using telephone booths.

Fast forward to 2015. Today I do my banking on my cellphone while watching a documentary at home and pay my way through life using the same cellphone. I check my official e-mail on my cellphone and play music in the car from my cellphone. I chat with my clan, college friends, neighbours and colleagues and exchange information in real time from my cellphone.

Technology brings new opportunities to tackle life and business challenges. But these opportunities come at a cost and new risks. These risks need to be managed effectively while ensuring that we gain the maximum benefit out of our technology investments, while keeping our data safe. From savings books to cloud computing and big data, the Government has not been left behind.

The Government of Kenya computerisation efforts of the last two decades are now starting to have a direct impact on Wanjiku. In line with cutting edge technology, government systems are starting to integrate and talk to each other. Early this year, I was able to renew my driving license online without having to leave my desk. I also managed to renew my passport online and only had to visit the Immigration Department for them to take my current photo. This is a great step forward for accessing government services. It is a clear indication that the Government is indeed serious with digital service delivery. In this regard, the launch of the e-citizen portal which brings together multiple Government agencies in one pane of glass is a huge step in the right direction. This has been adequately complemented by the Huduma Centres which are coming in handy for those citizens who may not be very digital savvy.

Since last year, The National Treasury has been rolling out the e-Procurement portal linked to the Integrated Financial Information Management System (IFMIS), through which all Government procurement has been put online. E-procurement has also been rolled out to County Governments, Parastatals and public Universities. The benefits of this to the tax payer are immense in terms of the efficiency and accountability that it brings. One of the biggest challenges to this and other Government systems is user acceptance, especially by Government officers in some quarters who were used to the old ways and other players who may want to scuttle these efforts for their own pecuniary gains.

The other challenge is security. While implementing cyber security is a resource intensive activity, organisations soon find out that to not implement is even more costly. The starting point of implementing a cyber security program is situational awareness. Currently, there is a criminal investigation going on regarding an alleged theft of public money at the National Youth Service where about Ksh 700 million is alleged to have been stolen by NYS officers in collusion with Ministry officers and suppliers, through the IFMIS system. The investigation of this cyber crime will bring to the fore the capacity situation for cyber crime and computer forensics investigation in Kenya, both at the investigating agencies and in the judicial system. The IFMIS system in this case will greatly help in terms of the inbuilt application security mechanisms by way of providing logs and an audit trail regarding the transactions. Gone are the days of lost files.

While many Government agencies have rolled out world class systems to deliver services to citizens, the current focus is now on building capacity to manage these solutions and also to increase the capability maturity of these systems. Of great importance in this regard will be performance management so that the Government can be able to clearly measure progress against key performance indicators in system implementation and integration, a key component of IT Governance.

The ICT Authority is doing a commendable job in this regard with their efforts to ensure that standards are followed, drawing from private sector skills and experience, as well as fast tracking more advanced training to develop a larger pool of IT Engineers with requisite skills. One area they may need to give closer consideration is the faster adoption of shared services especially in the area of Cyber Security to bridge the resource gap.

Government Sector Analysis

1

86% of government organisations are concerned by cybercrime.

86%

Agree cybercrime is a real issue

2

33% DON'T apply risk management in a bid to mitigate cyber-crime.

33%

DON'T apply risk management

3

85% allocate LESS THAN 500K annual on cyber security initiatives.

85%

Allocate **LESS** than Kshs.500,000

4

93 % DON'T know of the existence of Computer Emergency and Response Teams (CERTs) or their role.

93%

DONT know WHAT a CERT is

5

98% of government organisations are convinced that they are protected from cyberattacks internally while **94%** government organisations are not adequately protected from external attacks

98%

BELIEVE that they are protected from **internal attacks**

while

94%

Are **NOT** adequately protected from external attacks

Cyber Security Perspective from the Healthcare Services Sector

Collins Ng'eno | *Chief Information Officer, Nairobi Hospital*

The past decade has seen an increased growth in application of ICT in Kenya by healthcare providers such as hospitals, specialist clinics and medical insurance providers.

While there are tremendous benefits in terms of care delivery and organisational efficiency from the expanded use of networked technology; adoption of technologies such as connected medical devices, cloud networks and personal health devices has introduced new vulnerabilities.

Unlike industries such as finance, which have already been transformed by technology, many organisations in the healthcare industry have not invested sufficiently in robust ICT security measures that can protect health data, interfaces, repositories, databases, connected medical devices or personal devices.

The emergence of electronic health records (EHR), mobile applications and online portals has made it easier for patients and providers to access and share information. EHRs contain massive amounts of personally identifiable information which makes it very attractive to cyber criminals. It is estimated that globally stolen medical information costs up to 10 times more than credit card information in the black market, because unlike credit card information whose usefulness is limited to the validity period of the card, medical data is static and even if the breach was discovered there would be no way of invalidating the information.

In January 2015, the Government of Kenya announced a partnership with a leading multinational as a key technology partner for a wide-scale radiology infrastructure modernization program. This program is aimed at transforming 98 hospitals across Kenya's 47 counties through a comprehensive, wing-to-wing solution package that will see modern radiology equipment available in public hospitals across the country.

The biggest challenge that this and other similar programs face is availability of qualified radiologists to read and interpret the images on site due to the shortage of specialist doctors in the country. It's against this backdrop that we have seen the birth of tele-radiology services in Kenya, where medical images are transmitted over the internet to a radiologist for purposes of reporting.

The process is completely web based. Once a radiographer (technician) in the hospital or clinic performs an examination, the information is sent via a secure network to a team of radiologists who interpret the examination and the report is sent back to the hospital.

The above development will definitely increase the amount of medical information held or transmitted electronically in the country. Cybersecurity will therefore no longer be an option or an after thought, but a critical strategic agenda that the healthcare providers in the public and private sectors should incorporate in their existing governance, risk management and business continuity frameworks.

Healthcare organisations can no longer ignore the risk of cyber-attacks which has largely been associated with financial institutions in the past. We are likely to see an increase in the frequency of attacks in the future and the financial and legal consequences will become more damaging.

With no immediate answers in sight for organisations' tight security budgets and the limited ICT security talent pool, managed security providers would offer an ideal partnership for many organisation. Such partnerships will help address existing security gaps and provide customized solutions aligned to the organisations' business strategy.

Managed solutions deliver many benefits ideally suited for healthcare security concerns and deserve a closer look from any healthcare provider ready to address the challenges that lie ahead.

Economy & Politics
State to roll out cheaper off-peak power
Page 6

County Business
Pilot breathes life into sleepy Nanyuki airstrip
Page 12

Life
Careful steps for moderating a panel
Page 27

BUSINESS DAILY

A NATION MEDIA GROUP PUBLICATION NO. 1980 MONDAY, DECEMBER 1, 2014 WWW.BDAFRICA.COM KSH60 | TZ SH 1,700 | UGSH2,700 | RFr900

Kenya Facebook users lose millions in hacking scam

Local internet security firm says more than 5,000 accounts on the social media platform were breached

BY MUGAMBI MUTEGI

More than 5,000 Kenyan Facebook users have lost millions of shillings in a hacking scam that lasted for a year, a local cyber security firm has revealed.

The firm, Serianu, says it has unmasked a Kenyan hacker who broke into personal accounts of Facebook users in Nairobi, Mombasa and Eldoret and used the access to solicit funds from thousands of people linked to the breached accounts.

"The hacker created a website that looked aesthetically similar to Facebook and posted it on random users' pages, inviting them to view their friends' latest photos," said William Makatiani, the managing director.

"Users who clicked on the link were asked to provide their log-in details afresh in order to proceed. Once they did this, their usernames and passwords were collected into a database that currently has 5,006 entries."

The cyber criminals then used the captured log-in credentials to take over a user's social media page and went on to solicit money from the account owner's friends while masquerading as the real user.

Owners of the compromised Facebook accounts were also contacted and informed that their accounts would be deleted if they declined to pay money -- ranging between Sh5,000 and Sh100,000 -- into different mobile money accounts.

To nudge victims into paying up, the fraudsters posted malicious and alarming messages on breached Facebook pages. Serianu estimates that victims of the attacks may have lost up **HACKING, Page 4»**

BRIEFING

Safaricom reveals interest in cashless fare company

Safaricom has revealed that it has a commercial interest in the cashless fare payment card dubbed My 1963, which puts the telco among the biggest beneficiaries of the new system.

Page 8»

NEWS INDEPTH

Kenya shifts focus to high-risk groups in fight against HIV/Aids

Pages 16-17 »

TOP NEWS

Kenya Facebook users lose millions in hacking scam

»From Page 1

to Sh50 million in the scam. The hackers used fake websites to retrieve usernames and passwords of Facebook users, a practice referred to in technology jargon as phishing.

The *Business Daily* cannot reveal the hacker's identity or the website used in the scam because the matter has since been reported to the CyberCrime Unit of the Directorate of Criminal Investigations (DCI), who are investigating.

The website, which has since been taken down, was registered by a Kenyan, hosted locally and with a Safaricom mobile phone number as the contact line.

Internet security breach has become a serious problem since Kenya installed broadband Internet with the landing of undersea fibre optic cables in Mombasa five years ago.

Criminals have used high-speed Internet to illegally obtain and share crucial user information that has cost millions of companies and individuals billions of shillings annually.

UK broadcaster, BBC, last week reported that administrators of a Russian-based site infiltrated thousands of insecure baby monitors, webcams and CCTV cameras in over 250 countries, including Kenya, UK, Pakistan and Zimbabwe, and monitored live feeds.

In the past 12 months, there has been a build-up of Internet security breaches in Kenya. The Kenya Police and the Central Bank of Kenya top the list of 103 crucial government websites that have fallen prey to the hackers.

The Banking Fraud Investigations Department last year reported that hacking of customer bank accounts -- mainly by bank employees -- between April 2012 and 2013 led to losses of Sh1.49 billion.

Nairobi Senator Mike Sonko's Twitter account was reportedly compromised this week, exemplifying the ubiquitous nature of the crime in the country.

> We are waiting for the victims to come forward and make a formal complaint
>
> DCI OFFICER

The Facebook hacker's operation has since been shut down with the help of PhishTank, a US-based anti-phishing site used by leading IT firms like Google, Yahoo and Mozilla to verify the safety of websites.

A DCI officer at the CyberCrime Unit in charge of the Facebook scam investigation confirmed that Serianu had filed a report detailing the hacking incident.

"Serianu approached us recently and provided information about the alleged crime, including details of one of the individuals who was affected," said the officer who declined to be quoted as he is not authorised to speak on ongoing investigations. "We are waiting for the victims to come forward and make a formal complaint," said the officer.

The *Business Daily* has established that one of the victims is a nurse at a local hospital. Her Facebook account, which is still under the hacker's control, was compromised in late October and her friends have since wired Sh17,000 to the fraudster's different M-Pesa accounts.

Stephen Wanjala, the victim's husband, said they had contacted the CID officer in charge of the investigation and were preparing to make an official statement. Cyber security experts say the exponential increase in the number of local hackers is not only a direct result of improved Internet infrastructure, but also a quest for fame and wealth.

Besides, Kenya does not have enough professionals who can effectively secure personal data or rebuff cyber-attacks.

"Expert hackers around the world are considered heroes and revered in many quarters," said George Njoroge, CEO of East African Data Handlers. "Some local hackers are after a similar status and if they can make some money while at it, the better. Ignorance on the part of users, including companies, and lack of expertise worsen the situation."

A hacker at work. Kenyan Facebook users have lost millions of shillings to hackers. FILE

The Kenya Cyber Security report released in June by Telecommunication Services Providers of Kenya (Tespok) showed that cyber-attacks more than doubled in the past year to 5.4 million. While previously many of the attacks came from abroad – especially China – the majority of the 1.8 million computers used were stationed locally, indicating that the attacks were from within.

Insider threat by employees were earlier this year ranked top in the list of cyber security risks faced by financial institutions, especially those that have embraced mobile and online banking.

Mr Njoroge cited an ongoing investigation where five employees of a local mid-tier bank are being investigated for stealing Sh280 million from their employer. The case is expected to move to court this month.

The accused allegedly tinkered with the core banking system authorisation protocols and moved the money out to several accounts through mobile money and Internet banking transactions.

US information technology giant IBM in August signed a deal with the government that will see it develop cyber security syllabus for new recruits joining the police service.

Currently, most cybercrime matters are handled by small a team of IT experts – the Kenya Computer Incident Response Team – based at the Communications Authority of Kenya.

The team's core duty is to liaise with other government and international bodies to tackle cyber-crime.

pmutegi@ke.nationmedia.com

FOR MORE ON THIS STORY SCAN THIS CODE OR LOG ON TO
www.businessdailyafrica.com01122014

Cyber Security Perspective from the Financial Services Sector

Edgar Mwandawiro | *Head of Risk at Gulf African Bank*

Cyber security remains a critical concern for the banking industry. Players in the industry have underscored the importance of securing corporate cyber assets through commitment of extra funding to improve cyber security. The last couple of years have seen an increase in industry expenditure with the singular aim of achieving effective cybersecurity operational and strategic controls and planning.

The quest to provide customer convenience and aggressive marketing by financial institutions has seen technology-enabled institutions continuously interface and integrate their internal systems with external party systems to leverage on a variety of business opportunities and operational efficiency. Uptake of cloud and managed services has seen financial institutions better manage their capital expenditure and concentrate on their core business of providing financial solutions and services. Mobile and internet banking services tailored to suite local and global customers have seen financial institutions invest heavily on e- channel platforms and on strategic partnerships with telecommunication players.

Naturally, this growth comes with corresponding cyber risks, which have to be managed. As financial institutions continue to invest in complex technology infrastructure, strong asset management principles must be implemented to ensure classification, ownership and protection of those assets. While individual entity asset protection is indispensable, collective, inter-party and industry related initiatives are crucial. An improvement in legislation surrounding cloud infrastructure, assets protection and digital forensics is urgently required.

Financial institutions are still suffering large cyber fraud incidents, which have resulted in direct financial loss through the loss of customer funds and confidential customer information, perpetrated by customers, insiders or outsourced partners. In response to this, many financial institutions have put in place vendor risk management policies to address outsourced partners' risks, conduct background screening for employees, and KYC for customers. These have improved their internal systems controls, and enabled these institutions to proactively monitor transactions and employee behaviour change dynamics as part of critical elements to remedy the current cyber fraud prone environment.

The Government Anti-Fraud authorities must play a more active and independent role while carrying out banking/financial fraud investigations and ensure cases come to conclusion on time to the benefit of the defrauded financial institutions and the ultimate customers.

As technologies continue to expand to meet customer demands, electronic access to customer information and data they continuously pose significant challenges but also opportunities for business development. Therefore, the ultimate test should be how to enable customers access their data securely, what kind of information will/should be accessible and when allowed, how to secure the data while at rest and/or in transit.

The success of all cybersecurity projects and strategies lies in setting the tone from senior management through establishment of enterprise cybersecurity policies which will build a strong foundation for cybersecurity principles, governance, guidelines, procedures and processes.

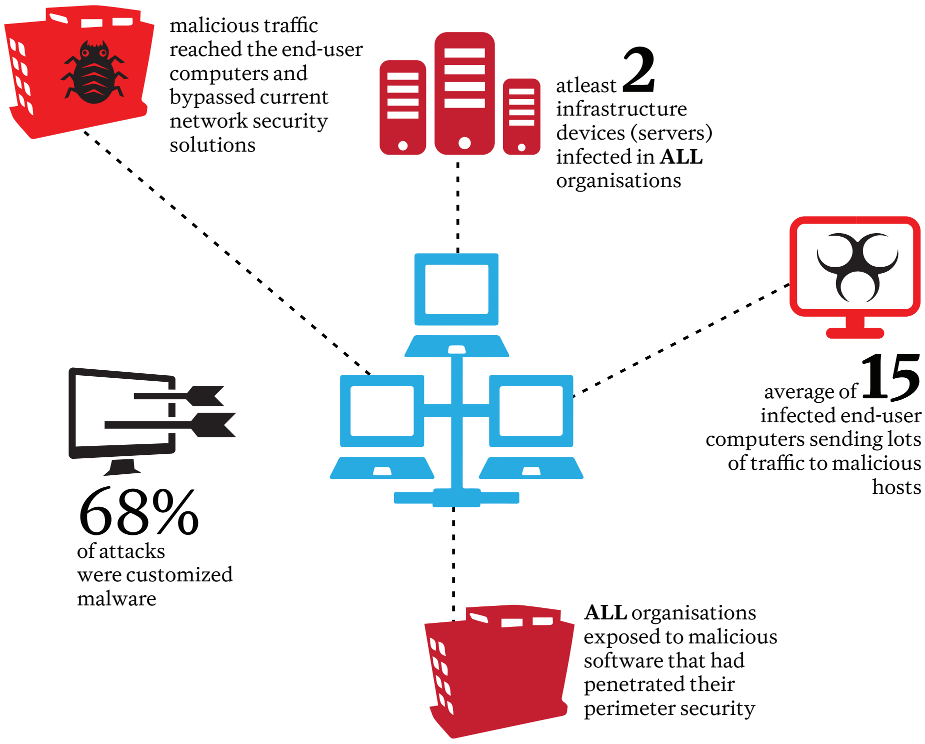
Kenya Cyber Intelligence Report

In this section of the report we share cyber threat intelligence from the Serianu Cyber Threat Command Centre - SC3. The section aims to provide an analysis of local cyber security threats, trends, and insights concerning malware, spam, and other potentially harmful business risks observed by the Serianu Cyberthreat Command Centre.

Serianu has established the most comprehensive source of Internet threat data in the country through the Serianu Cyber Threat Intelligence Network, which is made up of more than 10 monitoring sensors and records thousands of events per hour. This network monitors threat activity in Kenya through a combination of Serianu products and services such as Serianu Honeypot Network, Serianu Managed Security Services, and other third-party data sources.

For purposes of this report, we inspected network traffic inside a representative sample of Kenyan organisations. The goal was to find out whether there are malicious threats hiding inside the organisations' infrastructure that current information security solutions or practices do not detect or prevent.

We found that in all of the organisations, malicious traffic reached the end-user computers and was able to bypass the current network security solutions altogether. In all the organisations we identified atleast two infrastructure devices (servers) were infected and an average of 15 infected end-user computers which were sending lots of traffic to external IP addresses of compromised or malicious hosts - known as Command and Control servers.


malicious traffic reached the end-user computers and bypassed current network security solutions
atleast 2 infrastructure devices (servers) infected in **ALL** organisations
average of 15 infected end-user computers sending lots of traffic to malicious hosts
68% of attacks were customized malware
ALL organisations exposed to malicious software that had penetrated their perimeter security

Further, all the organisations in the study were exposed to malicious software that had penetrated the organisations perimeter security. Out of 300,000 security alerts, 68% percent were customized malware, 28% percent were trojans and 10% percent were backdoors. A customized malware is a malicious code that has not yet been seen by the internet security community.

How do you determine an infected organisation?

Normally, When a computer/host has been infected with malware, the malware will eventually start to call a remote server and wait for a response. These servers are also known as Command and Control servers (CnC). The attacker can connect to the compromised host via the CnC server and provide further instructions in order to conduct a targeted attack on the inside of the organisation network.

The main finding of the study is that all organisations in the scope of the study are already breached. It means that organisations in Kenya cannot trust that their information assets are secured.

According to this study, a typical Kenyan organisation is generating thousands of security incidents in a day, with the most active organisation generating around 10,000 security incidents per day. We have also discovered that organisations were averaging 2 infected infrastructure hosts (servers), 15 infected end user computers and 30 unauthorized remote connection per day.

Organisations should investigate whether their protection mechanisms are sufficient in today's interconnected world where attacks are growing in complexity.

Such figures illustrate how discouraging it is for Kenyan organisations to manually manage alerts in order to differentiate a real and present threat. There is a lot of malicious zero-day traffic that is impossible to detect using traditional information security solutions. In addition to this advanced threat, there is also known malicious traffic that should not exist if already installed solutions would work properly. It also sheds light on why recent high profile attacks at organisations, like the Sony Attack, were undetected for so long, since alerts don't equal infections. The only way to determine if an organisations has been compromised is to correlate logged activities, which takes way too much time and man hours.

Organisations should investigate whether their protection mechanisms are sufficient in today's interconnected world where attacks are growing in complexity

Cyber Security Perspective from the Manufacturing Sector

George Okwach | *Head of Audit, Crown Paints Limited*

There is surprisingly very little being done about cyber security in the manufacturing sector in the region. This lends from the notion that manufacturing's core business is too far hidden from the interest of cyber criminals. Manufacturing industry uses sophisticated software and other heavy ICT investments to drive their processes. Most of these systems are in the field of view of cyber criminals. Employee's behaviour through their interaction with the company's data and network using various devices, user accounts and passwords makes an organisation vulnerable to attacks.

There is need for the manufacturing industry stakeholders to pay more interest to the effects of cyber-crime in this sector through sharing of information on attacks, annual estimates of losses and how to mitigate cybercrime.

In Kenya and essentially the region, the issues of concern include;

1. How well proprietary assets like patents and formulations are protected. Most companies surprisingly spend tens of millions of dollars in marketing their products and almost nothing in keeping their patents safe from criminals. It doesn't take a casual intruder to run a second shift using your formulation secrets and scattering your top line.

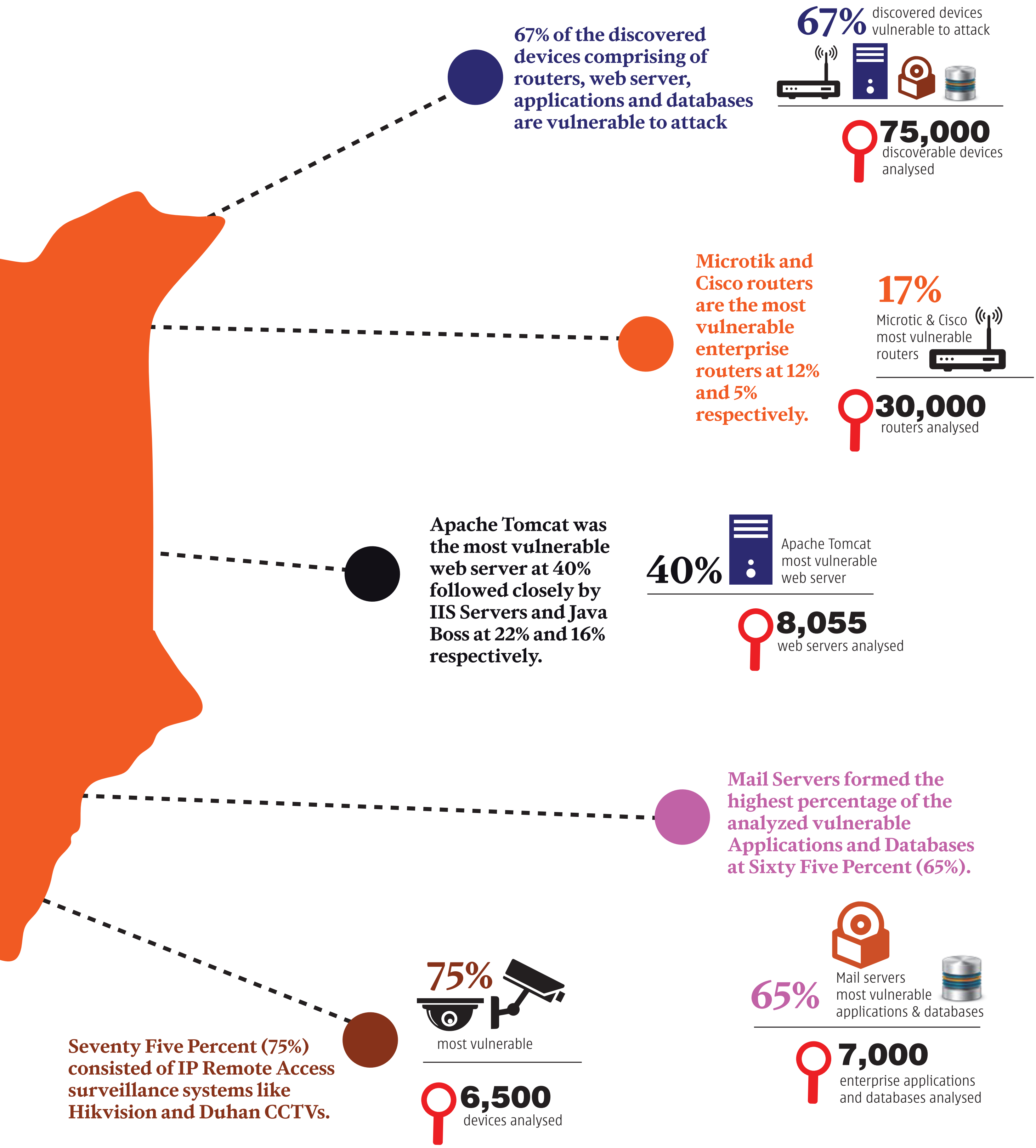
3. Assigning monitoring mechanisms to the systems, processes and people that manage your critical assets and information. It is wrong to think that once an SLA has been signed, penalty clauses will keep everything within bounds. The problem with this back seat approach is that promises fall below specifications and there are countless breaches on data and security without any of these being detected. Cyber criminals easily get away with crime because monitoring tools even if they exist are not being checked, users lack the know how of what to look for and most managers are just too busy with top line growth to bother.

4. Most companies in the region were founded on and continue to ride on cheap labour as a major incentive to invest. What we have seen in industry is employees learning a lot and using this knowledge for sinister acts.

5. Industrial warehouses that double as corporate headquarters often provide little access control mechanisms that distinguish the casual labourer/ contractor and a white collar techie. To "get the job done" managers and directors have given up bothering and have allowed intruders into sensitive areas and offices to their detriment. The information these intruders gather easily gets used for cyber and other crimes at costly consequences. In the current age of cyber Security, business owners need take a long term view and segregate Industrial plants and manufacturing areas from sensitive managerial desks where strategy and business development plans are negotiated and manipulated.

There is need for the manufacturing industry stakeholders to pay more interest to the effects of cyber crime in this sector through sharing of information on attacks, annual estimates of losses and how to mitigate cybercrime

Top Local Vulnerabilities



67% of the discovered devices comprising of routers, web server, applications and databases are vulnerable to attack

67% discovered devices vulnerable to attack

75,000 discoverable devices analysed

Microtik and Cisco routers are the most vulnerable enterprise routers at 12% and 5% respectively.

17% Microtic & Cisco most vulnerable routers

30,000 routers analysed

Apache Tomcat was the most vulnerable web server at 40% followed closely by IIS Servers and Java Boss at 22% and 16% respectively.

40% Apache Tomcat most vulnerable web server

8,055 web servers analysed

Mail Servers formed the highest percentage of the analyzed vulnerable Applications and Databases at Sixty Five Percent (65%).

65% Mail servers most vulnerable applications & databases

7,000 enterprise applications and databases analysed

Seventy Five Percent (75%) consisted of IP Remote Access surveillance systems like Hikvision and Duhan CCTVs.

75% most vulnerable

6,500 devices analysed

Top Local Network Threats & Vulnerabilities

Missing Patches

A patch is a piece of software designed to update a computer program or its supporting data, to fix a vulnerability or improve the program's functionality and performance. Missing software patches account for a majority of the Denial of Service and Remote Code Execution attacks Serianu identified to 2015.

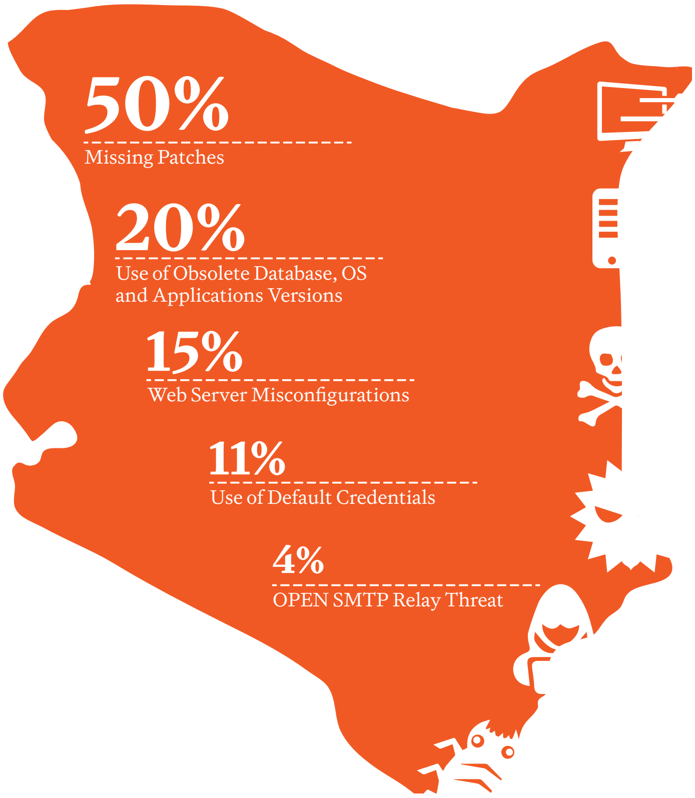
Majority of these organisations lack a patch management policy guiding them through the patching process.

Use of Obsolete Database, OS and Applications Versions

An obsolete version is one that is no longer supported by the vendor. The use of such systems therefore makes it easy for attackers to exploit since newly discovered vulnerabilities are not patched by the vendor. Some local organisations are using obsolete versions of MySQL and MSSQL databases as well as legacy operating systems such as Microsoft Windows Server 2003 and Microsoft Windows XP which are no longer supported by the vendor.

Web Server Misconfigurations

During our analysis, Serianu determined that the majority of local web server attacks are successful due to server misconfigurations. These misconfigurations include exposing sensitive web directories to the public, and leaving default server login pages active.



Use of Default Credentials

Default passwords pose a major security risk, as malicious individuals have access to this information on the Internet.

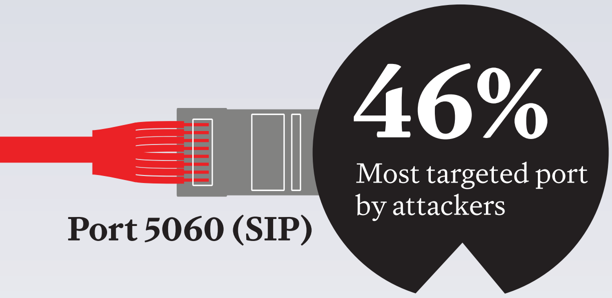
Once a user identifies a computer platform, all an unauthorized user must do is entering the default user credentials to gain access.

OPEN SMTP Relay Threat

An "open" SMTP relay is an SMTP server which allows mail to be sent without the need for authentication from aremoteuser. This vulnerability is exploited by malicious individuals who send fraudulent emails or use it for phishing scams.

It is common for these individuals to abuse open SMTP relays, sending thousands of untraceable messages through the server.

Top Attacked Ports



The port statistics show that at forty six percent (46%) port 5060 (SIP) was the most targeted port by attackers emphasizing the need to secure VoIP and IP Telephony solutions.

Cybersecurity Perspective from the Legal Advisory Sector

Anne Kinyanjui | *Partner, Iseme, Kamau and Maema Advocates*

Cyber-attacks are a threat to all businesses today and law firms are progressively becoming attractive targets to such attacks, particularly since they have confidential client information that could be of significant value to third parties. A law firm's reputation is perhaps its most valuable asset and clients expect all transactions and communication to be kept confidential. Maintaining this reputation in an era of increased cybersecurity breaches is critical, hence the need for firms to define the security controls required in order to mitigate against cyber-attacks. As the New York Times reported in 2014, **"a growing number of big corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount."**

Multinational corporations in particular, before issuing instructions, are requesting firms for information about their cybersecurity awareness, security protocols as well as the policies they have in place to safeguard client information. It is therefore important for firms to go beyond the traditional reactive mode and now become proactive in developing polices to protect information as well as enforcement mechanisms to enforce such policies.

Cybersecurity breaches take place at multiple penetration points. Some non-technical issues that need to be looked at as starting points include portable devices (BYOD) policies, desktop & workstation security, poor password protection, lack of encryption, employees lacking security awareness and weak controls & protocols for access to data (including remote access).

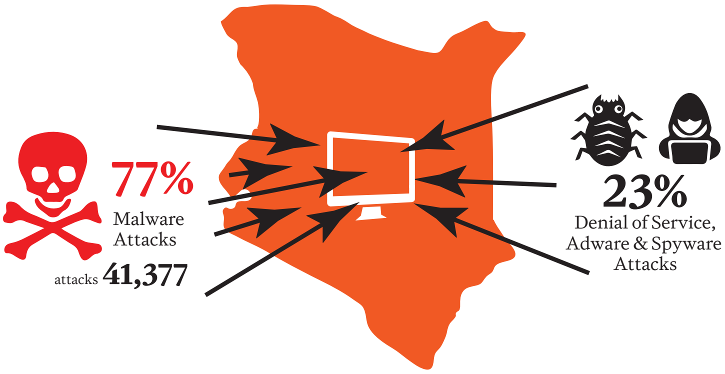
These risks can be mitigated in by building visibility around your data, assessing the risks posed to this data and developing appropriate security programs that focus on implementing cyber security policies and employee training and awareness.

These steps and others can help local law firms address their cybersecurity risks not just for maintaining their reputation and retaining client confidence but also as a key value proposition to differentiate themselves in the market place.

Kenya Cyber-Intelligence Statistics

Top Malicious Activity in Kenya

Malware attacks, Denial of Service (DOS) attacks and Adware attacks took the lead during this year's cyber security analysis in terms of volume.

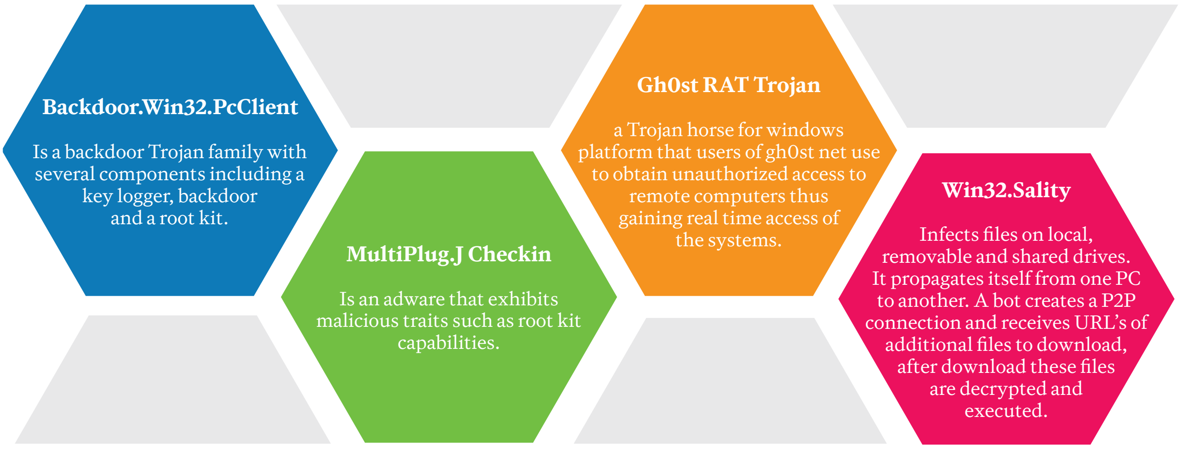


Malware Categories

68% of the malware category was uniquely customized for the African Region. The Virut malware is slowly penetrating the Kenyan cyberspace. Once it has successfully penetrated the computer, this type of malware is able to spread itself by copying to fixed, removable and network drives.

Customized Malware
68%

Local Malware Variants



Backdoor.Win32.PcClient

Is a backdoor Trojan family with several components including a key logger, backdoor and a root kit.

MultiPlug.J Checkin

Is an adware that exhibits malicious traits such as root kit capabilities.

Gh0st RAT Trojan

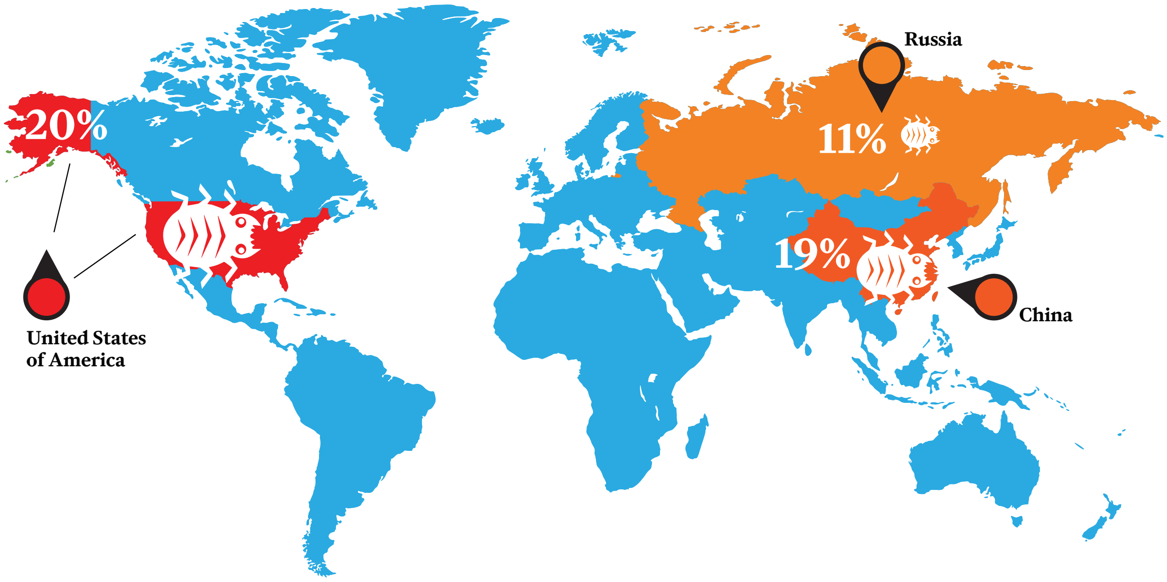
a Trojan horse for windows platform that users of gh0st net use to obtain unauthorized access to remote computers thus gaining real time access of the systems.

Win32.Sality

Infects files on local, removable and shared drives. It propagates itself from one PC to another. A bot creates a P2P connection and receives URL's of additional files to download, after download these files are decrypted and executed.

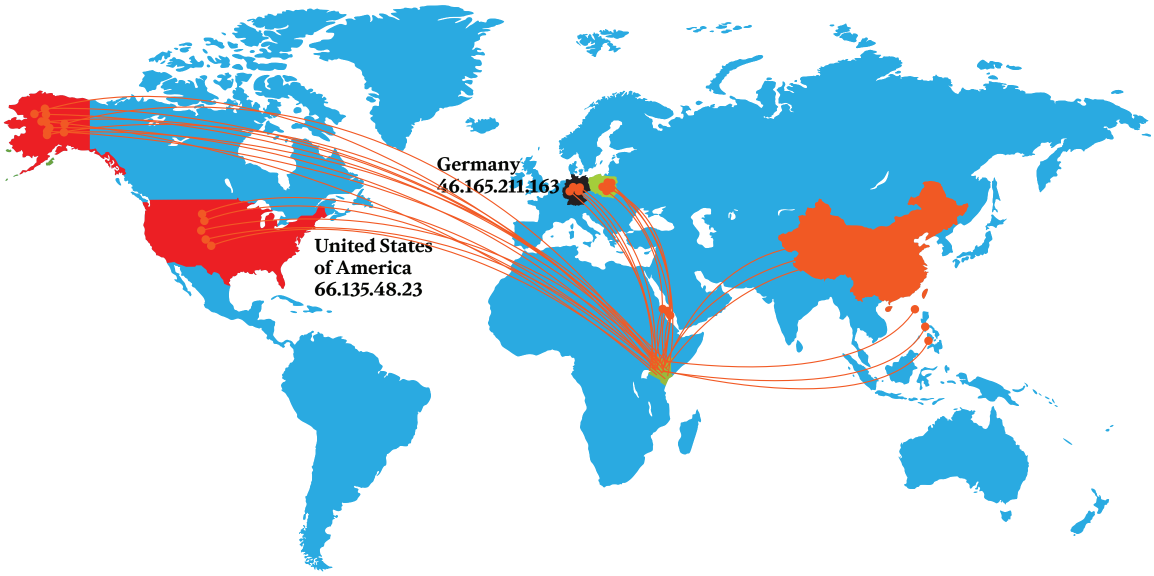
Top Malicious Countries

The top three malicious countries: USA, China and Russia formed the highest number of attacks targeting the Kenyan Cyber Space. Last year, USA came in third as a top attacking country, This year, USA came in first forming a fifth of the total attacks sent to Kenya NOTE: We understand the problem of attribution where there is a possibility to anonymize attacks using proxy and VPN services to make attacks look like they are originating from a different region.



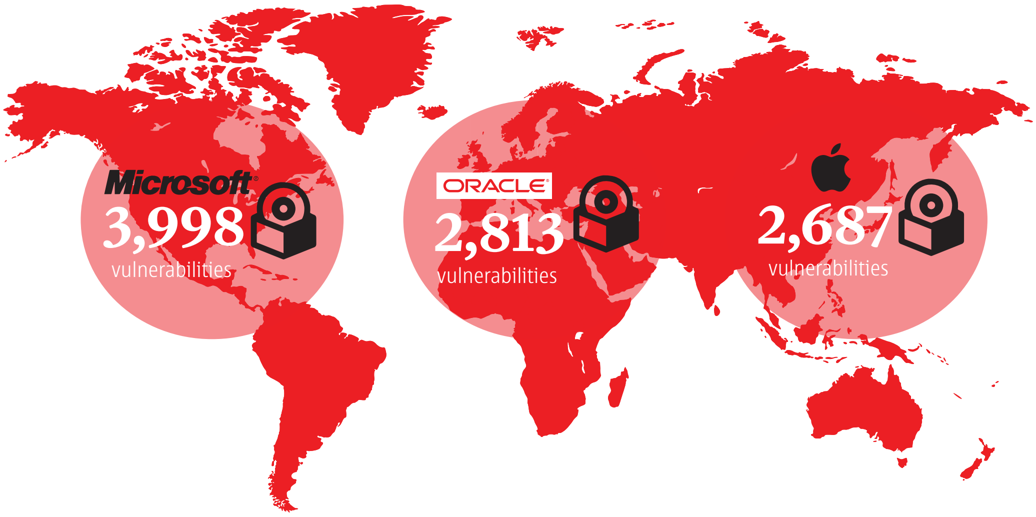
Top Attacking Global IP Addresses

Our statistics reveal that the top attacking IPs originate from the US, Germany and most recently, Serbia.



Global Threat Analysis

Microsoft, Oracle and Apple are the most popularly used application and operating system software platform in Kenyan organisations/homes. During our cyber security research period, we observed that Microsoft led all major technology vendors in identified vulnerabilities in its operating system and software with a total of 3,998 vulnerabilities followed closely by Oracle and Apple with 2,813 and 2,687 respectively.



Vulnerabilities vs. Exploits

During our analysis, we noted a dramatic increase in the total number of vulnerabilities and exploits between the year 2013 and 2014. Total number of vulnerabilities grew by 35% while that of exploits grew significantly by 53%.

Vulnerabilities

2013	2014
5191	7946

35% increase

Exploits

2013	2014
185	391

53% increase

Cybersecurity Perspective from the Insurance Sector

George Kisaka | *Head of ICT Audit, Britam Insurance*

Cybercrime Assurance Rather Than Insurance

Cybercrime is not a foreign thing anymore and regional governments have finally woken up to this realization. In the last year there have been efforts to review legislation and draft bills or set up government agencies and task forces to confront it. The Cybercrime and Computer Related Crimes Bill 2014 in Kenya and the Cyber Crime Act 2015 in Tanzania are testament to this.

The number one motive for cybercrime is financial gain, which puts insurers and other financial service firms at the greatest risk. A report by the Center for Strategic and International Studies, a Washington-based think tank in 2014, estimates the annual cost to the global economy from cybercrime to be more than US$400 billion. The report then and puts the financial services sector 2nd behind energy & utilities in annual cybercrime cost.

The Insurance sector has for long been a tech-laggard, a status that it could be argued has in a way shielded it from cybercrime. However, the banking sector has blazed trails in demonstrating how a focus on technological innovation, through evolving advances such as online and mobile banking, can be a real game-changer, and the insurance sector is slowly joining the bandwagon. Partnerships between insurers and the traditional banking sector in offering insurance cover, under the Bancassurance model, was just the beginning and the notable trend in the Kenyan insurance industry now is undoubtedly mergers and acquisitions (M&A). The trend is as a result of the search for growth and the upcoming regulations raising capital requirements within the industry and has led to bigger and more robust companies. To therefore get the upper hand, various companies are steadily adopting and leveraging on ICT to streamline operations, improve service, increase insurance penetration and grow margins.

As insurers continue to make forays into the internet, portals and mobile platforms, it is expected that cybercrime will spread into this industry too. Depending on the approach taken in adoption of ICT, it could have more far reaching consequences. Simply working with a core of the legacy systems in the background could be catastrophic as these may have limited capacity to withstand a cyber-attack.

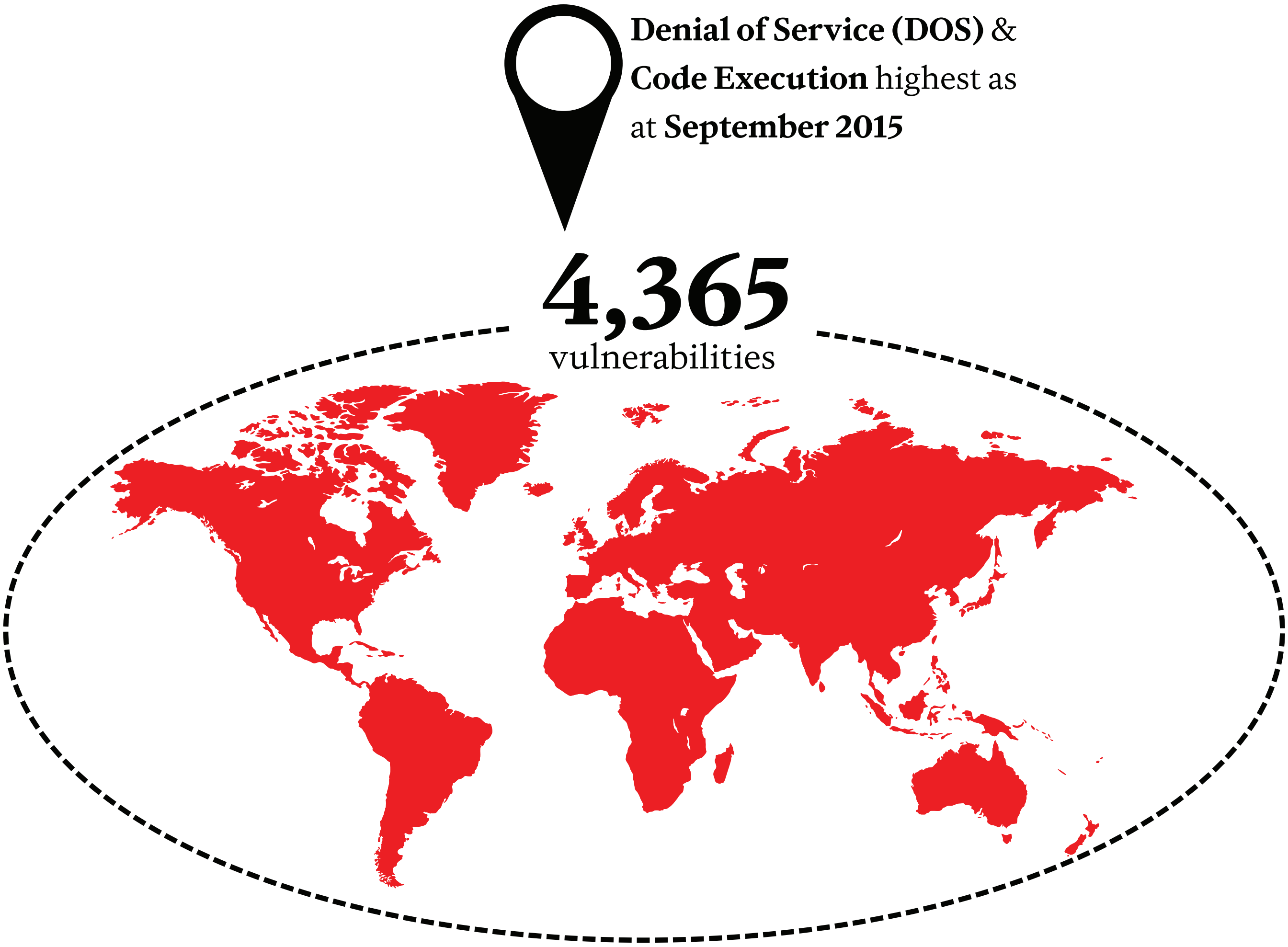
The insurance industry also finds itself included in the cybercrime debate not just as victims but as solution providers as well by underwriting cybercrime risk. This involves developing products to cover legal expenses, compensation, restoration and reputation costs among other things in case a company is attacked. Currently, cybercrime insurance is mostly sold in developed countries due to the complex underwriting and management it requires. Locally, uncertainty still exists on whether insurers have built capacity to comfortably offer cybercrime insurance given it is an emerging area. Most players are still grappling with questions relating to whether there is need, market and technical capacity (actuarial, underwriting, claims handling /processing, cybercrime risk mitigation etc.)

Going forward it is expected to pick up locally. We expect to see it begin with the local operations of larger global insurance companies that can leverage their experience in developed markets and sound financial backing before slowly being embraced by their local counterparts across the region. Indeed the first insurance cover against internet related crime was launched in Uganda in mid-2015. Given the prevalence of cybercrime, cyber-attacks are a question of when and not if. The topic here should then be **Cybercrime assurance rather than insurance**.

Top Global Software Vulnerabilities 2015

During our review, we noted a total of 4,365 vulnerabilities worldwide. Denial of Service (DOS) and Code Execution vulnerabilities featured as the highest vulnerabilities as at September 2015. Most of the systems affected by these two vulnerabilities were missing critical patches, whereas others had been misconfigured, thus exposing the systems to attack.

Majority of the web server attacks in the years 2014 and 2015 were caused by the successful exploitation of the top two vulnerabilities.



Denial of Service (DOS) & **Code Execution** highest as at **September 2015**

4,365
vulnerabilities

Serianu Cyber Security Framework

Over the years, Serianu has obtained extensive experience working with different SME and Sub-Saharan Africa- based organisations in an effort to implement information security programs. Most of these programs were based on global best practice such as ISO 27001/2, PCI DSS, NIST, COBIT.

Based on these experiences and industry wide consultations, we have noted that while compliance to these security standards is great and increases an organisation's credibility, it is quite a daunting and complex task. It requires discipline, proper documentation and enforcement of policies and procedures, deployment of the right tools and technology, on boarding of qualified and well trained information security professionals' and most importantly, support from top-level management.

Our experience working with organisations has enabled us to identify the challenges most African organisations face especially, the difficulty in determining risk exposure and the return on specific and general cybersecurity investments. Based on several studies and our experience we know that cost is the single biggest barrier to implementing adequate cybersecurity, particularly for smaller organisations.

As the 2015 report shows, most SMEs and African based companies of all sizes are unable to withstand cyber security attacks. In addition, most governments and critical infrastructure companies could be at risk from thousands of connections to smaller players whose implementation of the Global cybersecurity best practices may not be determinable. **The Serianu Cybersecurity baseline controls Framework identifies 4 core areas**: Cybersecurity Program Governance and Strategy, Vulnerability and Threat Management, User Provisioning and Access Management and Continuous Monitoring and Incident Response. Within these areas it drills down to a total of 14 categories.

Importantly, it will help small businesses in Sub-Saharan Africa to identify and prioritize specific risks and steps that can be taken to address them. It also identifies some of the most relevant threats and barriers to successful risk management. It is particularly helpful to small and medium-sized businesses seeking to implement the Global frameworks (NIST, PCI DSS, ISO 27001 and SANS Controls), breaking down more complex categories and analysis into 14 controls that simplify analysis and implementation.

Organisations intending to be compliant to any of the information security best practices should also be prepared to invest heavily in time and money. Over Kshs.50Millionis spent to assess the scope of the particular standard and in meeting its requirements. All this in an effort to safeguard an organisation's infrastructure from cybercrime both internally and externally.

The reality however, not all organisations are ready to invest millions of shillings to implement cybersecurity controls. Most organisations we have come across are not ready to spend millions of shillings to ensure compliance with these global standards. Nevertheless, it is imperative that the confidentiality, integrity and accountability of their information assets is protected.

In order to assist such organisations, we have developed these minimum baseline controls which when implemented by business operating in the sub-Saharan region will significantly reduce cyber-related security incidences, enable IT security proactively monitor activities on their key ICT infrastructure, provide the assurance that business operations will resume in the appropriate time in case of an attack or disruption etc.

The Framework

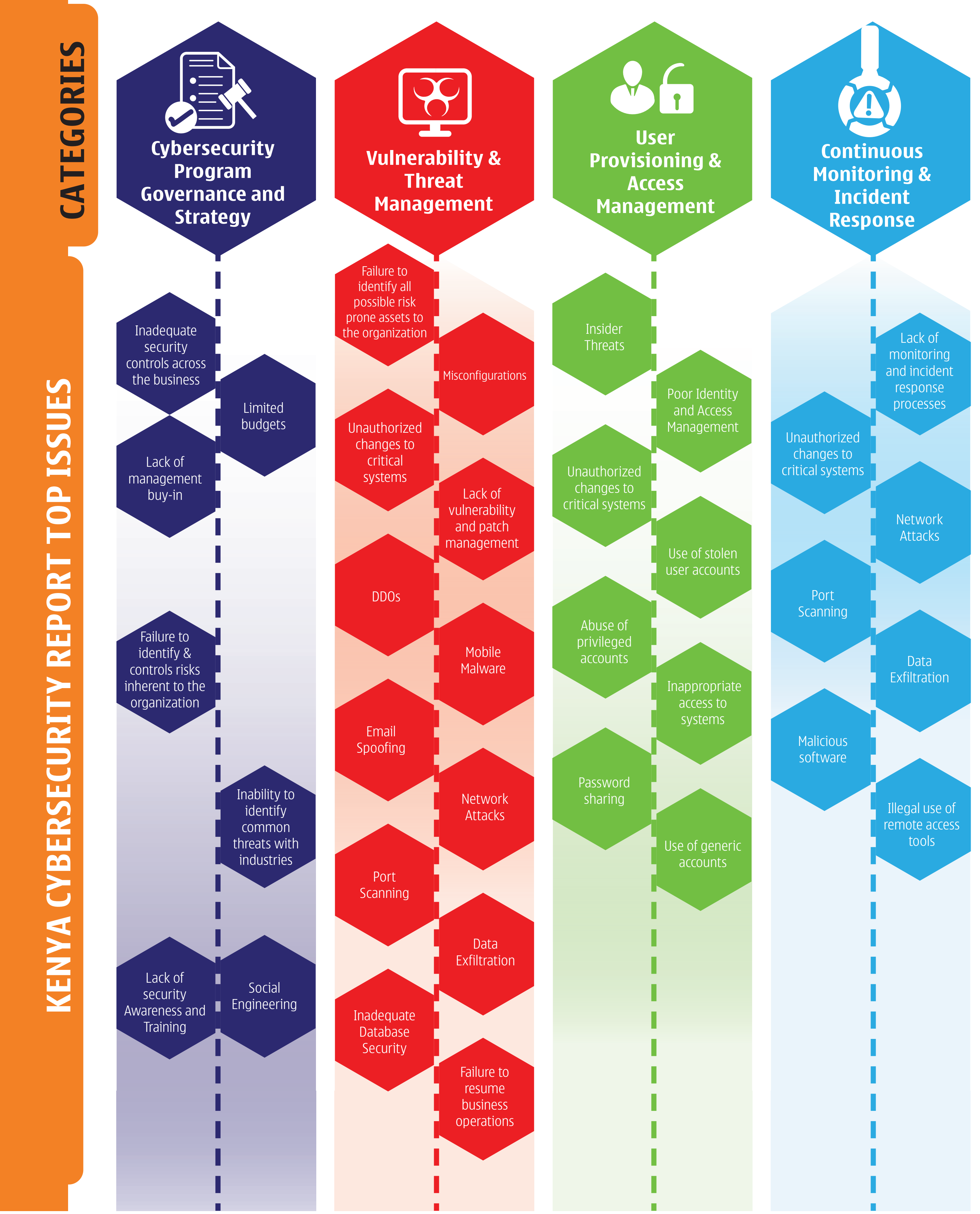
The Serianu Cybersecurity baseline controls are intended to address only the implementation and management of cybersecurity practices associated with information technology and operational consideration for organisations operating in Sub-Saharan Africa.

Serianu Cyber Security Framework is not intended to replace other cybersecurity-related activities, programs, processes, or approaches that organisations operating in sub-Saharan African have implemented.

These controls are designed to be flexible enough to be used both by SME and sub-Saharan Africa based organisations with mature cybersecurity and risk management programs and by those with less-developed programs. Each organisation will choose if, how, and where it will use the Framework based on its own operating environment. Choosing to implement the Framework does not imply that an existing cybersecurity and risk management approach is ineffective or needs to be replaced. Rather, it means that the organisation wishes to take advantage of the benefits that the Serianu Cyber Security Framework offers. This framework is closed tied to globally acceptable standards including COBIT, ISO 27001, SANS 20 Controls, and NIST.

This section highlights Serianu's 14 baseline controls. We have also matched the top threats and risks activities observed in the year 2015 as per the Kenya Cyber Security report to these controls.

The Serianu Cyber Security Framework



CATEGORIES

KENYA CYBERSECURITY REPORT TOP ISSUES

Cybersecurity Program Governance and Strategy

- Inadequate security controls across the business
- Limited budgets
- Lack of management buy-in
- Failure to identify & controls risks inherent to the organization
- Inability to identify common threats with industries
- Lack of security Awareness and Training
- Social Engineering

Vulnerability & Threat Management

- Failure to identify all possible risk prone assets to the organization
- Misconfigurations
- Unauthorized changes to critical systems
- Lack of vulnerability and patch management
- DDOs
- Mobile Malware
- Email Spoofing
- Network Attacks
- Port Scanning
- Data Exfiltration
- Inadequate Database Security
- Failure to resume business operations

User Provisioning & Access Management

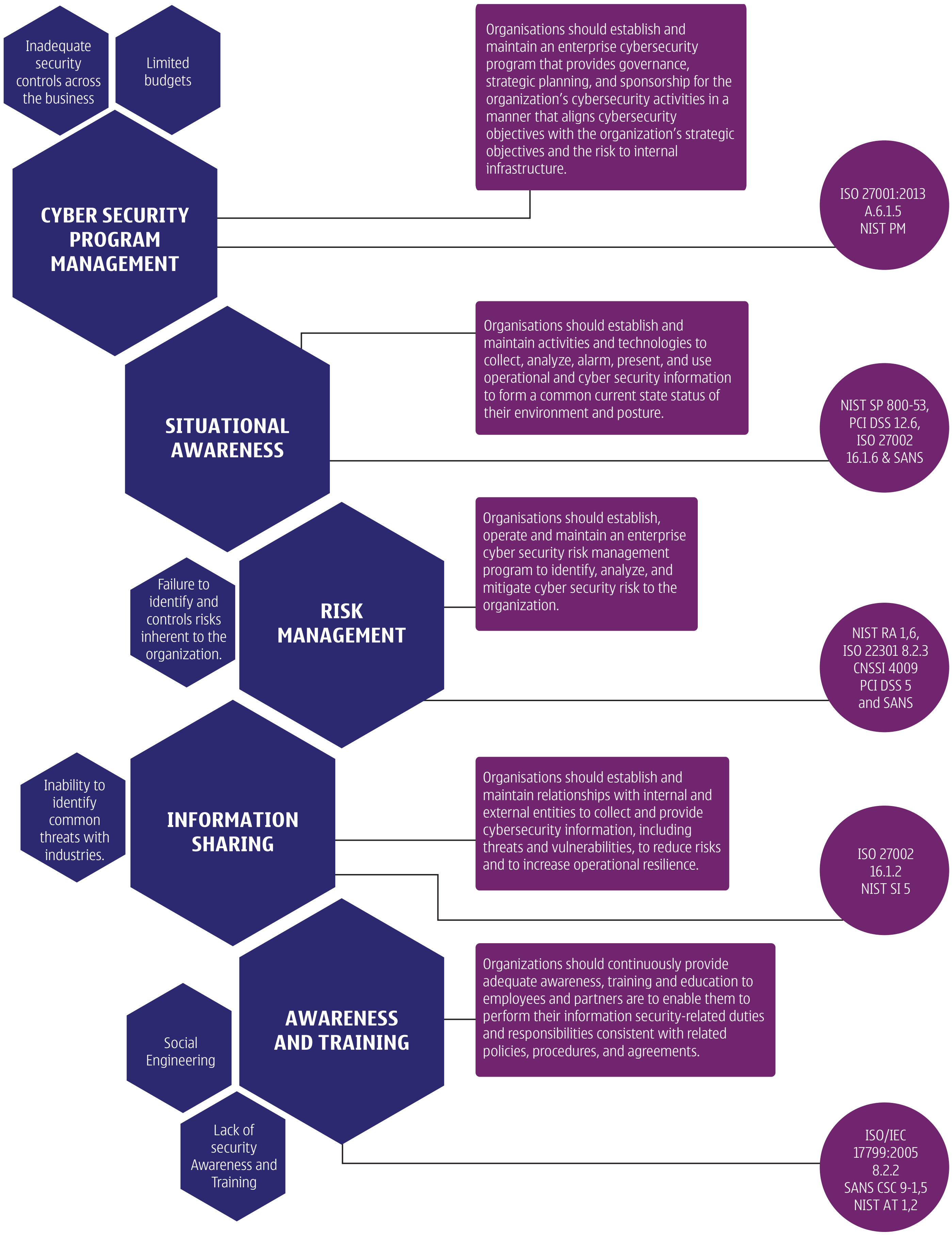
- Insider Threats
- Poor Identity and Access Management
- Unauthorized changes to critical systems
- Use of stolen user accounts
- Abuse of privileged accounts
- Inappropriate access to systems
- Password sharing
- Use of generic accounts

Continuous Monitoring & Incident Response

- Lack of monitoring and incident response processes
- Unauthorized changes to critical systems
- Network Attacks
- Port Scanning
- Data Exfiltration
- Malicious software
- Illegal use of remote access tools

Cybersecurity Program Governance and Strategy

CONTROLS | **Definitions** | **Global Frameworks Referenced**



Inadequate security controls across the business

Limited budgets

CYBER SECURITY PROGRAM MANAGEMENT

Organisations should establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with the organization's strategic objectives and the risk to internal infrastructure.

ISO 27001:2013 A.6.1.5
NIST PM

SITUATIONAL AWARENESS

Organisations should establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cyber security information to form a common current state status of their environment and posture.

NIST SP 800-53,
PCI DSS 12.6,
ISO 27002
16.1.6 & SANS

Failure to identify and controls risks inherent to the organization.

RISK MANAGEMENT

Organisations should establish, operate and maintain an enterprise cyber security risk management program to identify, analyze, and mitigate cyber security risk to the organization.

NIST RA 1,6,
ISO 22301 8.2.3
CNSSI 4009
PCI DSS 5
and SANS

Inability to identify common threats with industries.

INFORMATION SHARING

Organisations should establish and maintain relationships with internal and external entities to collect and provide cybersecurity information, including threats and vulnerabilities, to reduce risks and to increase operational resilience.

ISO 27002
16.1.2
NIST SI 5

Social Engineering

Lack of security Awareness and Training

AWARENESS AND TRAINING

Organizations should continuously provide adequate awareness, training and education to employees and partners are to enable them to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

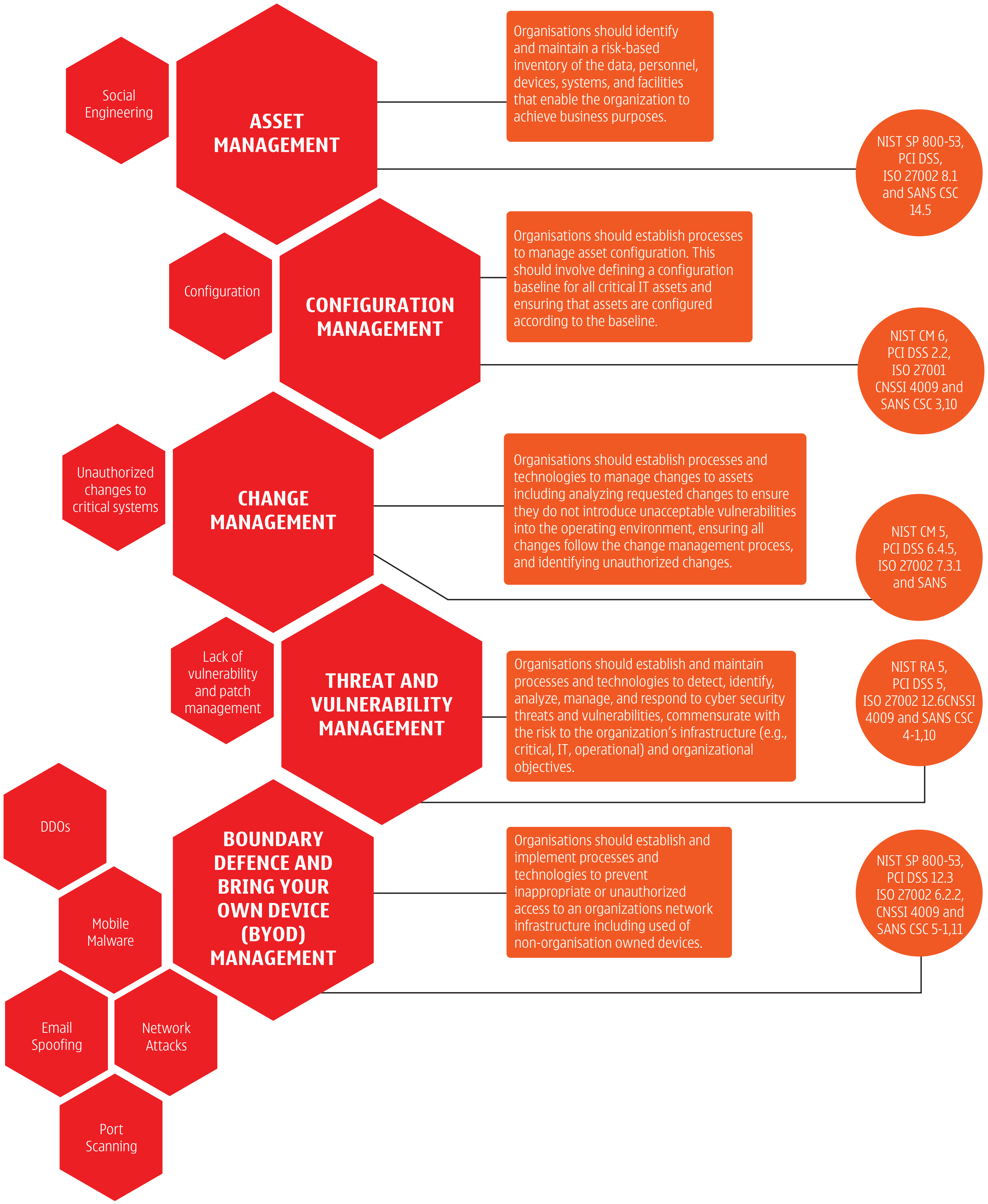
ISO/IEC
17799:2005
8.2.2
SANS CSC 9-1,5
NIST AT 1,2

Vulnerability & Threat Management

CONTROLS

Definitions

Global Frameworks Referenced



Social Engineering

ASSET MANAGEMENT

Organisations should identify and maintain a risk-based inventory of the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes.

NIST SP 800-53, PCI DSS, ISO 27002 8.1 and SANS CSC 14.5

Configuration

CONFIGURATION MANAGEMENT

Organisations should establish processes to manage asset configuration. This should involve defining a configuration baseline for all critical IT assets and ensuring that assets are configured according to the baseline.

NIST CM 6, PCI DSS 2.2, ISO 27001 CNSSI 4009 and SANS CSC 3,10

Unauthorized changes to critical systems

CHANGE MANAGEMENT

Organisations should establish processes and technologies to manage changes to assets including analyzing requested changes to ensure they do not introduce unacceptable vulnerabilities into the operating environment, ensuring all changes follow the change management process, and identifying unauthorized changes.

NIST CM 5, PCI DSS 6.4.5, ISO 27002 7.3.1 and SANS

Lack of vulnerability and patch management

THREAT AND VULNERABILITY MANAGEMENT

Organisations should establish and maintain processes and technologies to detect, identify, analyze, manage, and respond to cyber security threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.

NIST RA 5, PCI DSS 5, ISO 27002 12.6CNSSI 4009 and SANS CSC 4-1,10

DDOs

Mobile Malware

Email Spoofing

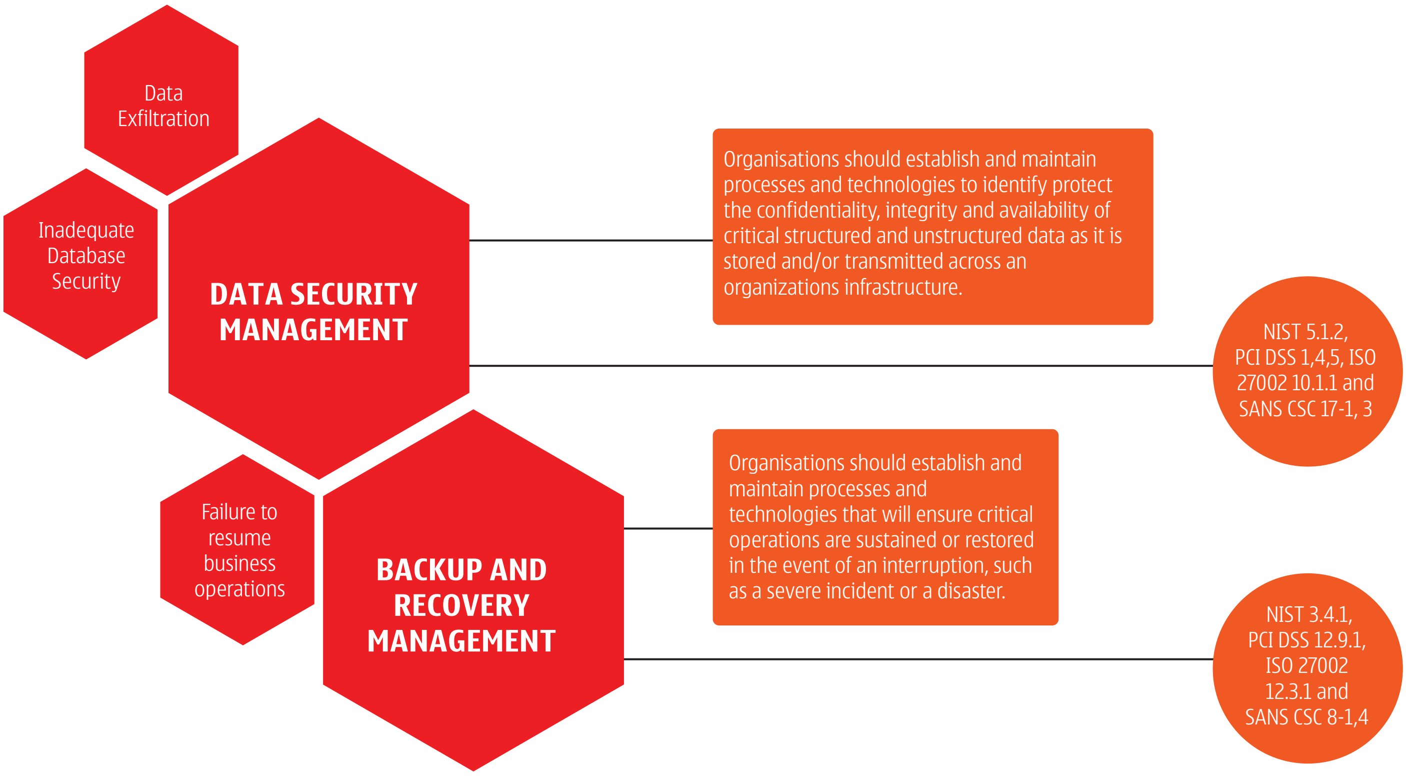
Network Attacks

Port Scanning

BOUNDARY DEFENCE AND BRING YOUR OWN DEVICE (BYOD) MANAGEMENT

Organisations should establish and implement processes and technologies to prevent inappropriate or unauthorized access to an organizations network infrastructure including used of non-organisation owned devices.

NIST SP 800-53, PCI DSS 12.3 ISO 27002 6.2.2, CNSSI 4009 and SANS CSC 5-1,11



Data Exfiltration

Inadequate Database Security

DATA SECURITY MANAGEMENT

Organisations should establish and maintain processes and technologies to identify protect the confidentiality, integrity and availability of critical structured and unstructured data as it is stored and/or transmitted across an organizations infrastructure.

NIST 5.1.2, PCI DSS 1,4,5, ISO 27002 10.1.1 and SANS CSC 17-1, 3

Failure to resume business operations

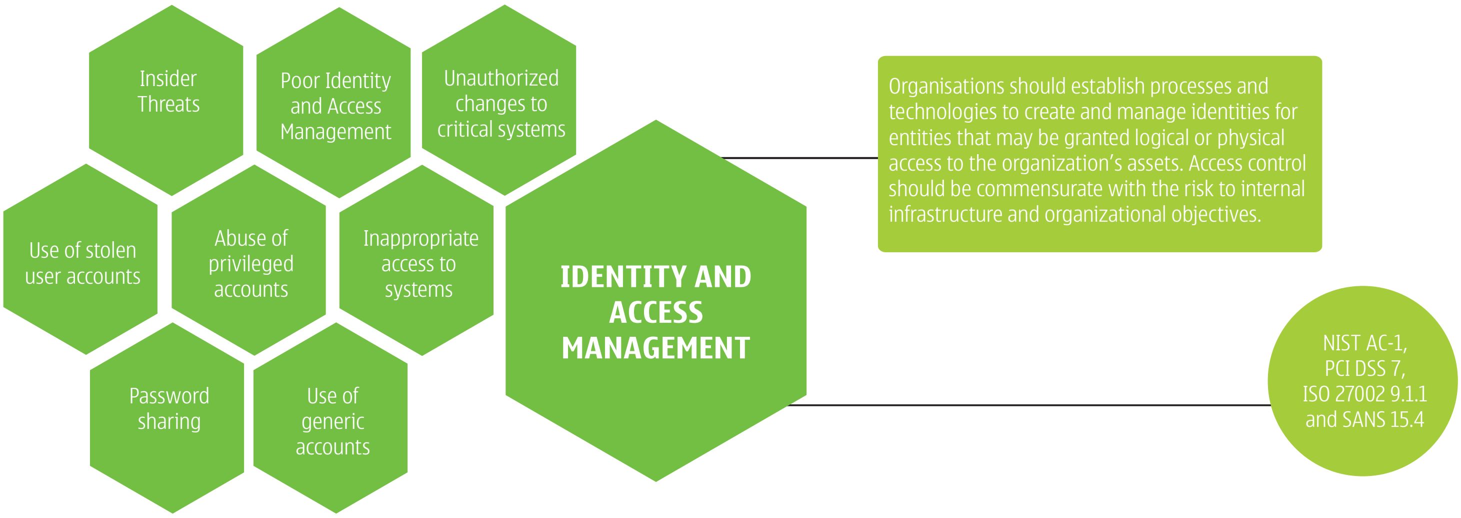
BACKUP AND RECOVERY MANAGEMENT

Organisations should establish and maintain processes and technologies that will ensure critical operations are sustained or restored in the event of an interruption, such as a severe incident or a disaster.

NIST 3.4.1, PCI DSS 12.9.1, ISO 27002 12.3.1 and SANS CSC 8-1,4

User Provisioning & Access Management

CONTROLS	Definitions	Global Frameworks Reference



Insider Threats

Poor Identity and Access Management

Unauthorized changes to critical systems

Use of stolen user accounts

Abuse of privileged accounts

Inappropriate access to systems

Password sharing

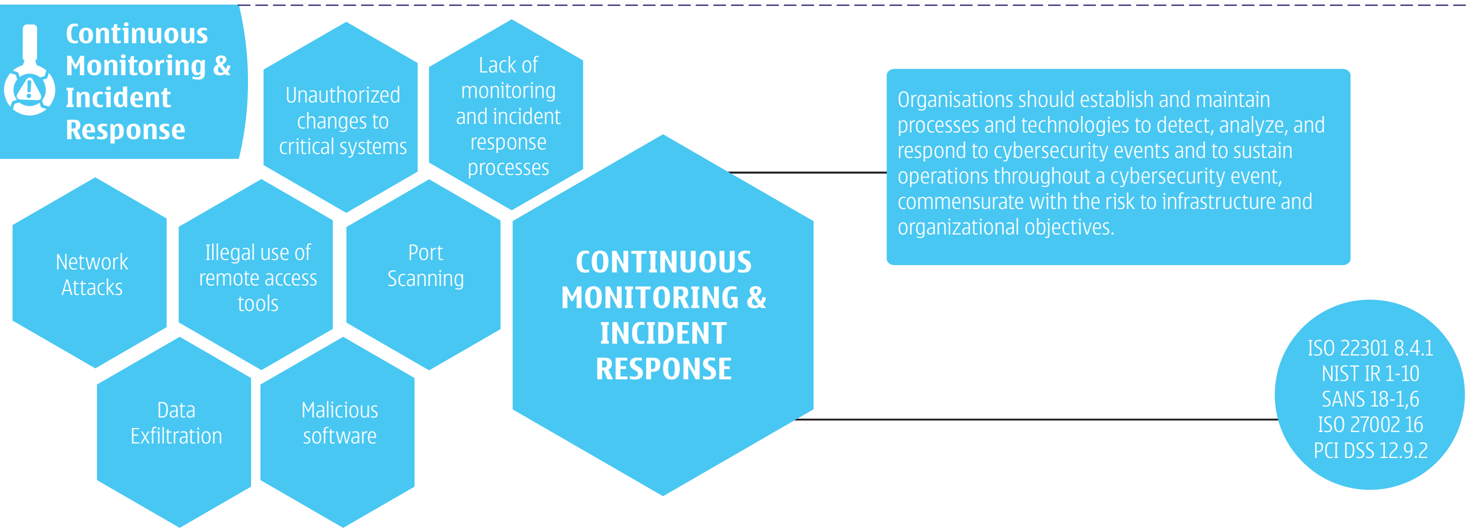
Use of generic accounts

IDENTITY AND ACCESS MANAGEMENT

Organisations should establish processes and technologies to create and manage identities for entities that may be granted logical or physical access to the organization's assets. Access control should be commensurate with the risk to internal infrastructure and organizational objectives.

NIST AC-1, PCI DSS 7, ISO 27002 9.1.1 and SANS 15.4

Continuous Monitoring & Incident Response



Unauthorized changes to critical systems

Lack of monitoring and incident response processes

Network Attacks

Illegal use of remote access tools

Port Scanning

Data Exfiltration

Malicious software

CONTINUOUS MONITORING & INCIDENT RESPONSE

Organisations should establish and maintain processes and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to infrastructure and organizational objectives.

ISO 22301 8.4.1
NIST IR 1-10
SANS 18-1,6
ISO 27002 16
PCI DSS 12.9.2

References

Cloud Computing

https://en.wikipedia.org/wiki/Cloud_computing

http://www.itnewsafrica.com/2014/09/cloud-computing-set-for-massive-growth-in-sa-kenya/

ERP Automation

http://www.automationmag.com/software/erp/1069-erp-success-mitigating-failure-risks

https://en.wikipedia.org/wiki/Enterprise_resource_planning

Managed Services

http://heartlandtechnologies.com/blog/7-advantages-managed-it-services

https://en.wikipedia.org/wiki/Managed_services

Mobile and Internet Banking

http://www.cnbc.com/2015/10/01/kenya-launches-first-mobile-only-m-akiba-government-bond.html

Commercialization of Hacking

http://blog.brightstores.com/2014/04/18/the-commercialization-of-hacking-software/

Regulatory & Compliance requirements

https://www.perficient.com/Industries/Financial-Services/Regulatory-Compliance

BYOD

https://www.sophos.com/en-us/security-news-trends/security-trends/byod-risks-rewards/what-byod-means-for-security.aspx

http://www.crn.com/slide-shows/security/240157796/top-10-byod-risks-facing-the-enterprise.htm/pgno/0/1

Teleworking

http://onlinecareertips.com/2015/04/benefits-and-disadvantages-of-teleworking-an-employees-perspective/

http://www.webopedia.com/TERM/T/teleworking.html

Internet of Things

http://www.webopedia.com/TERM/I/internet_of_things.html

http://www.kachwanya.com/2015/04/30/interent-of-things-in-kenya/

NFC

http://www.nearfieldcommunication.org/benefits.html

http://www.nearfieldcommunication.org/nfc-security-risks.html

http://www.digitaltrends.com/mobile/nfc-explained/

http://www.nfcworld.com/2014/05/16/329210/safaricom-reports-merchant-adoption-mobile-money-point-sale/

https://securityintelligence.com/is-nfc-still-a-vulnerable-technology/

Cyber Insurance

http://www.computerweekly.com/news/2240202703/An-introduction-to-cyber-liability-insurance-cover

http://www.insurancegateway.co.za/Kenya/PressRoom/ViewPress/URL=Cyber+liability+v+Commercial+Crime+Insurance+1#.Vgz0Svmqqko

Cyber Security Survey

https://www.cyberroad-project.eu/en/project/

http://www.cert.org/incident-management/national-csirts/national-csirts.cfm?

https://www.cvedetails.com/vulnerabilities-by-types.php

https://www.giac.org/paper/gsec/317/default-password-threat/100889

ATM Csoc

attack

Risk detection VPM infection

virus CBK Regulations

spam

terrorism

nation

resilience ring router child

malware

infection cyberspace PORTAL Risk

Virtual private network (VPN) copyright Reputation damage

Insider/disgruntled employee detection terrorism

Firewall DMZ COBIT Cyber criminal

Audit SPAM trojan

Honeypot Spyware

virus

DAM BYOD Phishing States Outsourcing DAM

Risk

Cyber Security

PORTAL ISO 270001 DDoS crime Encryption

resilience Csoc Hacktivist

intrusion prevention system spam Intrusion detection system (IDS) Virtual private network (VPN)

two-factor authentication Cyber Threat Personal firewall

websites pornography social engineering organised

offensive computers Business disruption

DMZ Financial fraud enterprise Cyber Threat

social engineering

Audit

virus defense

access

attack

Botnet

port

SERIANU CYBER-THREAT COMMAND CENTRE
SC3
DETECT • RESPOND • CONTAIN

PKF

USIU AFRICA
United States
International
University-Africa

HN/P