KENYA CYBER SECURITY REPORT 2014

Rethinking Cyber Security –
"An Integrated Approach:
Processes, Intelligence and Monitoring."

TESPOK

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

Acknowledgements

Authors

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

Christian Kisutsa
Information Security Consultant – Serianu Limited

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

Contributors

Fiona Asonga
CEO, TESPOK

Barry Apudo
Technical Manager, TESPOK

Joseph Muga
Network Engineer, TESPOK

Johnstone Ngugi
Research Associate

Gabriel Mathenge
Research Associate

Grace Gathoni
Research Associate

Tyrus Muya
Head of Information Security and Risk, Cellulant Group, Kenya

Joseph Mathenge

Senior Manager Information Security, Equity Bank, Kenya

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

Contents

Executive Summary

Foreword

Technology adoption is driving business innovation and growth in Kenya, at the same time it is exposing the country to new and emerging threats. Cyber-terrorists, spies, hackers, and fraudsters are increasingly motivated to target our ICT infrastructure due to the increasing value of information held within it – driven by our growing dependence on them – and the perceived lower risk of detection and capture in conducting cybercrime as compared to more traditional crime.

In the last couple of years; our ICT infrastructure has undergone a dramatic transformation. The growth in the use of systems and networks to connect various organizations has made it relatively easy to obtain information, to communicate, and to control these systems across great distances.

As a result of the tremendous productivity gains and new capabilities enabled by these networked systems, we have incorporated them into a vast number of applications and into virtually every sector of the country's critical infrastructure (government, IT, energy, water, food, and financial services). This revolution in connectivity has increased the potential for those who would do harm, thus making it is possible for a malicious agent to penetrate millions of computers around the world in a matter of minutes.

Spyware, Social Media, Peer-to-Peer networking, Phishing, unsecured email, loss and theft of mobile computing devices and cell phones are a major source of cyber threats incidents globally and still get most of the media attention. However, more insidious and prevalent is the lack of risk management programs, poor engineering practices, unsecured application development techniques, and inadequate infrastructure design which are the root causes of security vulnerabilities.

In the past one year we have witnessed a huge rise in cyber-criminal activity targeting both public and private organizations in Kenya. Criminals are not just targeting our computers, they are targeting the information that the networks store and transmit. Whether the source of an attack is an insider, a hacker, or a terrorist, the consequences are often the same—loss of revenue, loss of sensitive information, erosion of consumer and constituent confidence, interruption or denial of business operations.

To successfully combat cyber-criminal activity - there is a need for organizations to rethink cyber security and adopt an Integrated Approach to fighting cyber-crime. Organizations need to define cyber security processes, develop better intelligence and continuously monitor our networks. There is also a need for the private sector and government to work together to understand emerging threats and to develop proactive security solutions to safeguard the Internet and physical infrastructure that relies on it.

The Kenya Cyber Security Report 2014 provides an open forum to discuss emerging threats, their potential impact and countermeasures for containing them.

After the report launch, we invite you to learn more about our work in cyber security and engage with our experts to understand and address the challenges we face in securing cyber space.

William Makatiani

Managing Director
Serianu Limited

About the Report

The Kenya Cyber Security Report 2014 was analyzed, compiled and published by the Serianu Cyber Threat Intelligence Team in Partnership with the Telecommunications Service Providers Association of Kenya (TESPOK ICSIRT) and 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 organization's network for malware and cyber threat activities such as brute-force attacks against the organization's servers.

In an effort to enrich the data we are collecting, we have partnered with The Honeynet Project ™ and the Polish CERT 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 Cyber Usalama 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 organizations. It is through this initiative that we develop free monthly cyber security alerts and quarterly reports in conjunction with TESPOK. The reports are available at the Cyber Usalama website **www.cyberusalama.co.ke.**

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.**

Industry Perspective

To give our readers an industry perspective, we have invited three industry players from different sectors to share their perspectives on the state of cyber security in Kenya.

Financial Sector – *Mr. Joseph Mathenge, Senior Manager Information Security, Equity Bank, Kenya*

Technology and Media – *Mr. Tyrus Muya, Head of Information Security & Risk, Cellulant Group, Kenya*

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

Financial Services Commentary

Mr. Joseph Mathenge

Regional organizations are now more than ever cognizant of the threat that cyber criminals pose to their Information and Communications systems. It is no secret that all leading industry players have invested heavily in technology systems and continue to leverage it as a strategic component in dominances over their sectors. This dependency comes however at a cost in that the heavy use of these technologies has created new avenues through which criminals and other malicious actors exploit.

In late 2013, Kenya's Information, Communication and Technology Cabinet Secretary, Fred Matiangi, released statistics that the country would lose an estimated KSh 2 billion (about US$23 million) through cybercrime. Uganda 2012-2013 annual Police crime and traffic report indicated a 14.9% surge in economic crimes - Cybercrime, which in the report focused on mobile money and Automated Teller Machine (ATM) fraud, was responsible for the loss of about USH 1.5 billion. According to Bank of Tanzania (BoT) statistics TZS 1.3bn has been stolen across the country through cyber fraud.

These losses are significant and regional governments have responded in creating public awareness as well as enacting laws to help investigate and prosecute this growing and worrying trend. We have seen steps to counter cybercriminals with the authorities forming specialized units to fight against the cyber-crime. Tanzania for example has formed a task force with members from Bank of Tanzania (BoT), Tanzania Communication Regulatory Authority (TCRA), Financial Intelligence Unit (FIU), Tanzania Bankers Association (TBA) and the Police Force Cyber Crime Unit. Kenya is in the process of drafting tough cyber laws. The draft,dubbed Cyber-Crime and Computer Related Offences Bill 2014, is to address offences against confidentiality, integrity and availability of computer data and systems. It also seeks to curb cyber stalking, hate speech and identity related crimes.

The private sector is certainly no bystander in this trend. Executive Management typically engages in discussions with their Enterprise Operational Risk leaders (Chief Risk Officers or similar) on strategic topics around protecting their information assets from cyber criminals. This I believe is a new trend. IT leadership are now more than ever required to provide reports on the overall systems security posture and what steps are being taken to mitigate known as well as unknown vulnerabilities

Industry spending is on the rise with organizations spending more of their technology budgets in buying more security tools to help automate and enhance the enterprise security posture. These tools range from the traditional Firewall and Antivirus solutions to advanced End Point protection, Web Application Firewall and Security Event Management (SEM) tools.

Some of the key issues that is fueling this change includes:

- Improving external/internal audit items. Enterprise risk board committees and senior management continue to ask tough questions around IT risk audit items and demand resolution to items identified.
- As government enact laws it becomes more critical to meet regulatory requirements –Kenya for example include a chapter on ICT risk in 2012 prudential guidelines. Banks are required to meet the requirements spelled out in this document.
- As discussed earlier there is a need to address traditional fraud vectors that are in use on new platforms. E.g. illegal funds transfer via Electronic Funds Transfer (EFT) that is simply the traditional check fraud now cloaked in electronic systems.

- Since more money is spent on new security tools organizational leaderships is demanding successful deployment, administration and maximize use of the solutions procured to protect information assets. This to properly show that the organization not only procures the right tools but that these tools are in use and yield the desired Return on Security investment.

To completely eliminate cybercrime is simply not possible at this time. Regional practices however have shown continuing maturity in handling the menace. A key capability that is required and must be developed is the ability to detect criminal activity early and a rapid response to minimize damage. Industry professionals and those charged with the responsibility of protecting information assets mustcontinue to use above key drivers to obtain Sr. management support. It is also very important to learn to speak to the business about the business opportunity created in maintaining secure and reliable systems. Most professional tend to focus only on the potential loss and practice the principal of FUD (fear, uncertainty and doubt) and miss the opportunity of secure systems as being a business growth driver. Finally note that it is impossible to know all the potential pitfalls and attack vectors that cyber criminals employ so in the famous words of Steve Jobs we should ***'Stay hungry. Stay foolish'*** and continual seek education, research to learn of industry direction.

Mr. Joseph Mathenge is a Senior Manager, Information Security at Equity Bank, Kenya.

Please note that the opinions expressed herein, belong to the individual and do not necessarily express the views or opinions of their respective employers.

Technology and Media Commentary

Mr. Tyrus Muya

Cyber security has become a recurrent theme in the ICT industry and more importantly in the last one year. The key highlight in Kenya was the development and launch of the National Cyber Security Master plan developed by the ICT Authority in collaboration with Booz Allen & Hamilton from the USA. This earmarked a firm commitment from the Government to establish pillars along which cyber security threats are addressed in support of emerging technologies and improved policy frameworks. Also of significant importance was the Public Key Infrastructure initiative which supports the master plan's core objective of secure transmission & protection of data.

From an industry perspective, 2013 saw an increase in financial fraud which affected a majority of banks through different vectors; ATM skimming, mobile banking, credit card theft and insider collusion. All these contributed to high financial loss while at the same time getting attention from industry regulators that more needs to be done in as far as oversight and legislation is concerned. Given the intricacies of eliciting a successful prosecution, legislators have an opportunity to develop laws with the times to curb this rising vice.

The past year has also seen information security threats shine the light on the efficiency of past and current methodologies in as far as IT security audit and assessments are concerned. Given the increase in threats going unabated, there has been a need to interrogate techniques and metrics used to benchmark businesses and organizations against a less reactive threat models. Research has gone into establishing models within which cyber security risks are addressed efficiently with minimum impact to the overall business objectives.

We have also seen an increase in collaborative efforts with learning institutions to close the gap in capacity building. Private firms have emerged leading the way in developing requisite skill sets with relevance to the constantly shifting security landscape. In my opinion, 2014 is a promising year to address known threats as well as model insights around seemingly innocuous threats e.g. information warfare, APTs, public infrastructure attacks (GSM: especially with the licensing of banks as Mobile Virtual Network Operators) and public utilities.

Mr. Tyrus Muya is the Head of Information Security & Risk, Cellulant Group, Kenya.

Please note that the opinions expressed herein, belong to the individual and do not necessarily express the views or opinions of their respective employers.

Academic Sector Commentary

Mrs. Paula Kigen

We celebrate the launch of yet another Kenya Cyber Security report. The efforts that go into the data collection, analysis and publication of this report are commendable and should be applauded. The content is specific to our country and region and this gives us more threat intelligence than we would obtain by reading reports from other regions of the world. If anything, local information security reporting is rare in Kenya let alone Africa as a whole. It is important to gain visibility into the local attack trends and share these insights with all stakeholders so that we can collectively rise above the challenges and secure our community better. As it is commonly said, security is only as strong as the weakest link.

The trends captured in this report are similar in many ways to global trends reported in other regions all over the world. For example, the challenges of Domain Name System (DNS) attacks and Distributed Denial of Service (DDoS) have been highlighted in other 2013 information security reports. This means that Kenyan information systems are not isolated from the larger internet community. It also means we can benefit for international efforts to secure ourselves. Continuing with the example, it means Kenyan organizations can take advantage of the DNSInspect (dnsinspect.com) and Open Resolver Project (openresolverproject.org) to test our DNS servers and see if they are susceptible to attack.

Malware and the Advanced Persistent Threat is yet another huge global challenge we are also witnessing in Kenya as shown in the report. The number of new malware samples identified is increasing exponentially worldwide with the new frontier being on mobile device platforms.

An interesting distinction however is that we are still grappling with malware and botnets that have been successfully put under control in other regions of the world. For example Cutwail/Pushdo and Kelihos infections continue to be high despite the existence of solutions to clean out infections.

The biggest challenge we face in this regard is lack of active research and co-operation among different members of the information security community such as CERTs, ISPs, government, private organizations and even academia to address the threat. Attackers also know this and are taking advantage of it.

Kenya also needs to have a definitive incident response team and active CERT to help the country recover in the event of a large-scale coordinated cyber-attack. The possibilities of such an attack are high and concerns of our preparation to address such a threat are not unfounded. As more of our population gets connected to the internet, and the more we depend on information systems for business and day-to-day life, the more devastating such an attack could be.

Lastly, there is a growing population of tech-savvy youth who are not gainfully employed and are seeking to make a quick buck, live lavishly and drive the latest cars. As they discover the vulnerabilities in our information systems and see ways of making money; we are only likely to see more information security threats and bigger losses for organizations and the economy. We need to work together to protect our information systems. This report is a great starting point to drive the dialogue and to strengthen our collaboration.

Mrs. Paula Kigen, is a Research Associate Director, Centre for Informatics Research and Innovation (CIRI) and the Digital Forensics and Cybercrime Lecturer, United States International University (USIU)

Please note that the opinions expressed herein, belong to the individual and do not necessarily express the views or opinions of their respective employers.

Defining Cyber Security

What is Cyberspace?

Cyberspace, while not existing in any physical form, is a complex environment resulting from the interaction of people, software and services on the internet by the means of technology devices and networks connected to it.The complex environment encompasses the interconnecting networks and systems as well as any ICT devices belonging to different organisations and service providers that allow for the flow of information

Cyberspace belongs to no one but has key stakeholders including:

- End Users
- Private and Public organisations
- Internet Service Providers (ISP)
- Government – Regulators and enforcement

What is Cybersecurity?

Cyberspace security or Cybersecurity refers to the security of the cyberspace, providing guidance to address issues arising from the gaps between different security domains in the cyberspace environment while at the same time providing an infrastructure for collaboration. Cybersecurity focuses on addressing the need for efficient and effective information sharing, coordination and incident handling amongst the four stakeholders.

Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

Cybersecurity is a necessary consideration for individuals and families, as well as businesses, governments, and educational institutions. For families and parents, online safety of children and family members is of significant importance. In terms of financial security, it is imperative to protect information that could impact our personal finances if in the wrong hands or exposed to malicious cyber criminals. By protecting our computers, we protect precious private files, documents and other media.

Small and medium-sized businesses face critical challenges due to limited resources and the constant pressure to address business priorities and meet business targets. The speed at which technology is evolving makes it difficult to stay current with security without proper processes and structures in place within the business. However, better security awareness and planning can help these businesses protect their sensitive information, intellectual property and trade secrets while reducing loss of productivity due to downtime.

What is Cyber insecurity?

Cyber insecurity on the other hand is the growing concern about the rise of cyber threats and the ability to defend oneself and mitigate risks in cyberspace. This usually occurs when vulnerabilities of computer systems are exposed, including flaws or weaknesses in both hardware and software, and individuals with access to them. It takes the forms of cyber warfare, espionage, crime, attacks on cyber infrastructure, and exploitation of computer systems. Everyone is exposed to the above mentioned activities if proper mechanisms and procedures are not in place to protect them or more so,they lack any precautionary measures to protect themselves online.

The consequences of cyber insecurity include but are not limited to the loss of critical and sensitive information, loss of revenue, violation of privacy, lack of access to legitimate online services, exposure to cyber-attacks and exposure to cyber fraud. These consequences have been experienced all over the world and more so right here in Kenya. This report gives in-depth insight to the state of cyber security in Kenya for the year 2013.

SERIANU

SERIANU CYBERTHREAT COMMAND CENTRE (SC³)

The Serianu CyberThreat Command Centre (SC³) monitors activities and events in client environments to ensure that anomalous behaviour is detected, identified, classified and acted upon where appropriate. Security engagements are co-managed where actionable behaviour is recommended in the event of malicious activity. Ongoing reviews of all activity and reports provide technical security oversight to detect meaningful data versus non-threatening anomalies. Client control environment procedures are also monitored to ensure that breaches of these procedures and the possible precursors of malicious activity are identified and reported.

PROTECT AGAINST MALICIOUS THREATS

The Serianu CyberThreat Command Centre (SC³) focuses on security and compliance. Security monitoring at Serianu guards your critical systems, seeking out any indicator of malicious activity from intruders that can threaten or even paralyze the very core of your business. Serianu will alert you immediately should a potential security breach be detected that could compromise the integrity of your network and can assist with remediation. It's a cost-effective, peace-of-mind solution to safeguard your network and your business' essential data.

Daily and monthly reporting provides the documentation required to demonstrate that threatening anomalies are detected and acted upon, while compliance also demands that all events have also been recorded and identified accordingly.

In the event of threats, Serianu provides actionable behaviour to counteract the event. Serianu will also provide forensics where appropriate, and maintain the proper evidence for legal action.

In order to successfully co-manage our clients' security, Serianu offers to assess our clients' environment to assist with defining the balance between security, compliance, best practices and budgetary constraints. Our Enterprise Security Services perform comprehensive testing and audits and provide the security solutions to protect your business-critical systems including:

The services offered by the SC³ allow us to identify, plan appropriate answers and react to cyber threats, often already installed within organisations' information systems:

- Event security monitoring
- Incidents detection and management
- Maintenance of systems in secure conditions
- Cyber Intelligence, threat and vulnerability monitoring
- A priori analyses of the compromised network and a posterior analyses of the extent of attacks
- Audits and tests (technical infrastructure)
- Crisis management assistance
- Security and footprints indicators provisioning

Section 1: Threat Landscape

In this section, we highlight the malicious activity observed in the year 2013. This data represents the malicious activity our sensors were able to identify. The significance of understanding this data is to provide insight towards what attacks are prevalent in Kenya, how the attacks are being carried out, which assets are being targeted and why, what is facilitating the attacks and most importantly gain some insight on the type of traffic to look out for in your corporate network.

1.1 Top Threats in (2013)

The Kenyan cyber security landscape is evolving fast as more organisations are becoming vulnerable to intrusions and exploitation. The fast-growing digitally-enabled operating ecosystem in Kenya is characterized by increasingly sophisticated insiders and outsiders launching more frequent and targeted attacks.

These attackers are using clever tactics to penetrate inherent weaknesses in information security programs and systems, rendering standard methods of detection and incident response obsolete. The list below gives an overview of the top threats in 2013.

1. Insider Threats

Insiders Threats remains the biggest security threat facing Kenyan organisations in 2013. In this period, insider threats contained a high incidence of deliberate malicious activity by current employees. Privileged users probed systems for unauthorized access, co-opted other user's access privileges, and attacked systems for a variety of reasons including disgruntlement, revenge, competitive advantage and blackmail. The scope of Insider Threats only intensified as business models continued to evolve with increased mobility, a growing mix of users, and geographically diverse business offices.

2. VoIP PBX Fraud

The introduction and increasing popularity of Internet Telephony (Voice over IP - VoIP) services has led to the majority of PBX's used in Kenyan organisations to have internet connectivity where traditionally they did not. This has increased the number of attack vectors available to be exploited where they have not been secured. A growing number of businesses in Kenya are being targeted by PBX fraud/hacking. This type of fraud has been around globally for the past 10-20 years; however over the past few years there appears to be a concerted focus on attacking businesses within Kenya. PBX fraud/hacking generally involve a third party making long duration international calls at the expense of a business. Hackers gain unauthorised access the business's PBX phone system and generate profit from the calls that they make to international premium rate numbers, leaving the business who owns the PBX phone system liable for payment.

3. Social media

Social media websites have become a popular platform that many Kenyan organisations use to build new relationships and contacts. However, social media websites are also being used by cyber criminals to indulge in various cyber crimes. In 2013, the number of criminal offences related to social media websites in Kenya increased. Most of these cases we identified were related to posting of defamatory, hate speech, cyber-bullying, obscene matter or images on various social media websites. During the Westgate terror attack of 2103, the terrorists utilized social media such as twitter to gain information on the rescue efforts being conducted by the police.

4. Denial of Service attacks

The continued growth of new online services launched by organisations in Kenya is increasing the country's susceptibility to targeted Denial of Service attacks. Many attacks are originating from compromised servers at hosting providers that are slow to respond to malware clean-up requests, as well as servers that are out of reach of international authorities. The government has introduced a number of online enabled services including; Integrated Financial Management Information System - IFMIS, iTax and KenTrade single window system. In the private sector

banks are introducing internet banking systems, insurance companies are introducing customer portals while other organisations are introducing customer case support and fulfillment systems.

5. Botnet Attacks

The number of compromised computers (botnet) in the Kenyan cyberspace is growing. In 2013, the number of botnet activity detected, increased by 100% from 900,000 events for the period ending December 2012 to 1,800,000 events for 2013. This is attributed to the increasing number of broadband and high speed internet subscriptions. These subscriptions are exposing new unsecured computers and routers to the internet - increasing the number of computers that can be compromised by cybercriminals. Once these devices are compromised, they can be used to spread viruses, generate spam, and commit other types of online crime and fraud. These attackers then utilize this highly distributed network to attack targeted infrastructure such as financial institutions and government ministries in attempts to defraud, cripple or steal information.

6. Online and Mobile Banking

The continued adoption of online and mobile banking services is leading to new threats for customers and local financial institutions'. Many financial institutions are introducing vulnerable web and mobile applications. In a recent study we sampled 33 online banking portals. Out of the 33 banking applications sampled, only 2 banking portals had adequate online security deployed on their web application. Majority of the web applications reviewed lack of strong encryption and are susceptible to phishing attacks.

7. Mobile Money Fraud

The continued popularity of Mobile money adoption in the region has attracted criminals who are now targeting this new money transfer channel. In 2013, we noted an increase in mobile money fraud targeting individuals and organisations. The fraudsters are getting innovative and a very fast on finding loopholes in new controls implemented by merchants, banks and consumers.

8. Cyber Espionage

In 2013, there was an increase in cases of cyber espionage. Cyber espionage refers to the stealing of secrets stored in digital formats or on computers and IT network. Cyber criminals either sponsored by states or individual organisations are using highly sophisticated and carefully constructed methods to gain access to a network and steal information quietly. Locally, there were reports that a local foreign embassy was targeted by a foreign government in an attempt to steal information. Cyber espionage is an emerging threat especially with the ongoing political and economic policy changes in the country. There is also the threat of competing organisations using cyber espionage attacks to gain information from their competitors.

1.2 Threat Landscape Analysis

In 2013 the number of cyber threat attacks detected in the Kenyan cyberspace grew by 108% to 5.4million attacks compared to 2.6 million attacks detected in 2012.

During the period we detected numerous attempts to penetrate cyber networks operating in Kenya. The attacks observed originated from the cyber space of a number of countries including Kenya. We also observed that the attackers were compromising computer systems located in Kenya and used masquerading techniques and hidden servers to hide the identity of actual system from which the attacks are being launched.

Anonymous Proxy server attack activity grew by 480%

The fastest growing cyber-threat was anonymous proxy servers located in Kenya. In the period under review, we detected a total of 290,000 attacks originating from anonymous proxy servers compared to 50,000 similar attacks in 2012. Anonymous proxy servers refer to computer systems that allow users to access the internet without leaving a footprint. Any cybercriminal can use these servers to attack other users in the Kenyan cyberspace with little or no likelihood of detection. Anonymous proxies are difficult to track and are especially useful to those who wish to hide their existence such as political dissidents and cyber criminals..

PBX Attacks activity grew by 73%

In the period under review the number of PBX (VoIP) attacks detected by our sensors increased by 73% from 450,000 attacks detected in 2012 to 780,000 attacks detected in 2013. During the same period there was a noted increase in the number of VoIP attack reports from local organisations. Many of the affected organizations realized that their VoIP servers had been hacked after huge bills from the VoIP service providers.

Botnet activity up by 100%

In 2013, the number of botnet activity detected, increased by 100% from 900,000 events for the period ending December 2012 to 1,800,000 events for 2013. A botnet is a collection of computers, connected to the internet, that interact to accomplish some distributed task. Although such a collection of computers can be used for useful and constructive applications, the term botnet typically refers to such a system designed and used for illegal purposes. Such systems are composed of compromised machines that are assimilated without their owner's knowledge.

Year	PBX Attack	Malware	Botnet	Proxy	Trojan
2012	450,000	1,000,000	900,000	50,000	200,000
2013	780,000	1,750,000	1,800,000	290,000	580,000
% increase	**73%**	**75%**	**100%**	**480%**	**290%**

Table 1.1: Threat Landscape 2012 vs 2013

In the period under review we noted an increased in cyber threats in Kenya.

Activity	Q1 2013	Q2 2013	Q3 2013	Q4 2013
PBX Attacks	120000	160000	200000	300000
Malware Attacks	300000	400000	450000	600000
Botnet Attacks	200000	400000	500000	700000
Proxy Attacks	50000	60000	80000	100000
Trojan Attacks	130000	150000	200000	300000
TOTALS	**800000**	**1170000**	**1430000**	**2000000**

Table 1: Threat landscape analysis

The table below shows the internet uptake in the country for the period 2012 to 2013.

	Q1 2013	Q2 2013	Q3 2013	Q4 2013
Terrestial Wireless Data/Internet subscriptions	24011	21282	17169	16429
Fixed Fibre optic data/internet subscriptions	55007	58197	61739	67470
Fixed DSL Data/Internet Subscriptions	10390	11512	11537	12014
TOTALS	**65397**	**69709**	**73276**	**79484**

Table 1.2: Internet uptake analysis courtesy of CCK

From our analysis it can be seen as the internet uptake increased, the numbers of attacks have also increased over the same duration. This is attributing to the increase of activity online which warrants the attention of cyber criminals.

chart on the next page >>>

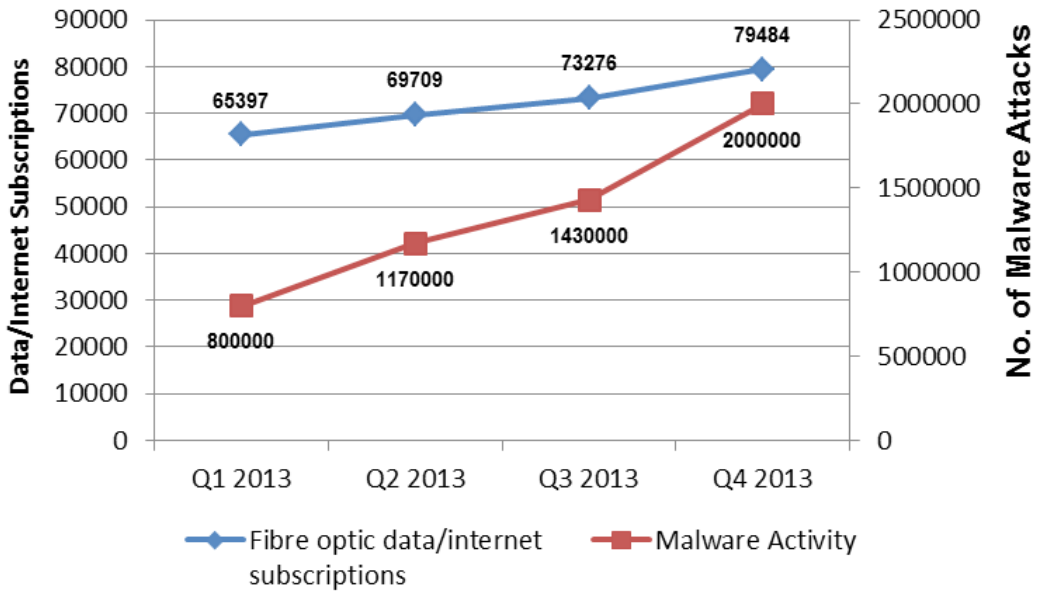


Chart 1: Threat Activity vs.Internet Usage in 2013

A. Malicious activity & attacks

Malicious Activity

The threat landscape in 2013 has been quite steep due to the amount of malicious activity observed through the year. Botnet activity comes in first followed by other types of malware and spamming.

Malicious Activity

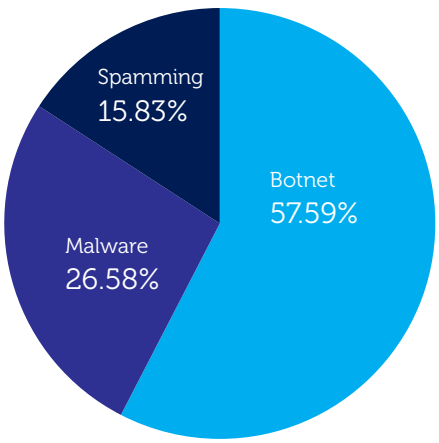


Chart 2: Malicious Activity

Malicious Activity

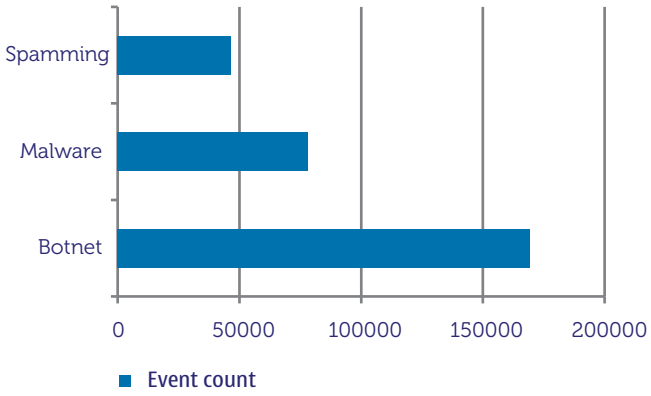


Chart 3: Malicious Activity

Top Attacks

Attacks	Percantage	Severity
Proxy attacks	62.30%	High
DNS attacks	28.90%	High
Web app attacks	7.41%	High
SSH attacks	0.89%	High
Phishing attacks	0.49%	High

Table 3: Top Attacks

The top 3 attacks of the year were Proxy attacks, DNS attacks and Web app attacks. Proxy servers are susceptible to attack due to poor configuration by the respective custodians of the identified asset. DNS attacks are more rampant as evidenced by consecutive attacks on local ISP's and Google. Web attacks on word press are identified on a day to day basis due to the rise in demand of online websites. Most of the sites are developed without a basic understanding of website security leaving clients with administration panels available to the public that can be readily attacked by brute force attacks.

Malicious Kenyan IPs		
IP Address	ASN	Country
212.49.74.210	AS12455	Kenya
41.72.206.234	AS33770	Kenya
41.223.57.99	AS36926	Kenya
41.206.60.158	AS15808	Kenya
212.49.64.45	AS12455	Kenya
41.215.124.117	AS15808	Kenya
41.203.219.198	AS37061	Kenya
41.222.11.222	AS36866	Kenya
41.76.170.13	AS37219	Kenya
212.49.64.17	AS12455	Kenya
196.201.226.66	AS36866	Kenya

Table 3(b): Malicious Kenyan IPs

Table 3(b) above highlights the top malicious Kenyan IP addresses through the year 2013. These IPs perform regular wide spread host scans of well-known ports among other malicious activity such as brute force attacks and exploit attempts.

Malicious Kenyan IPs

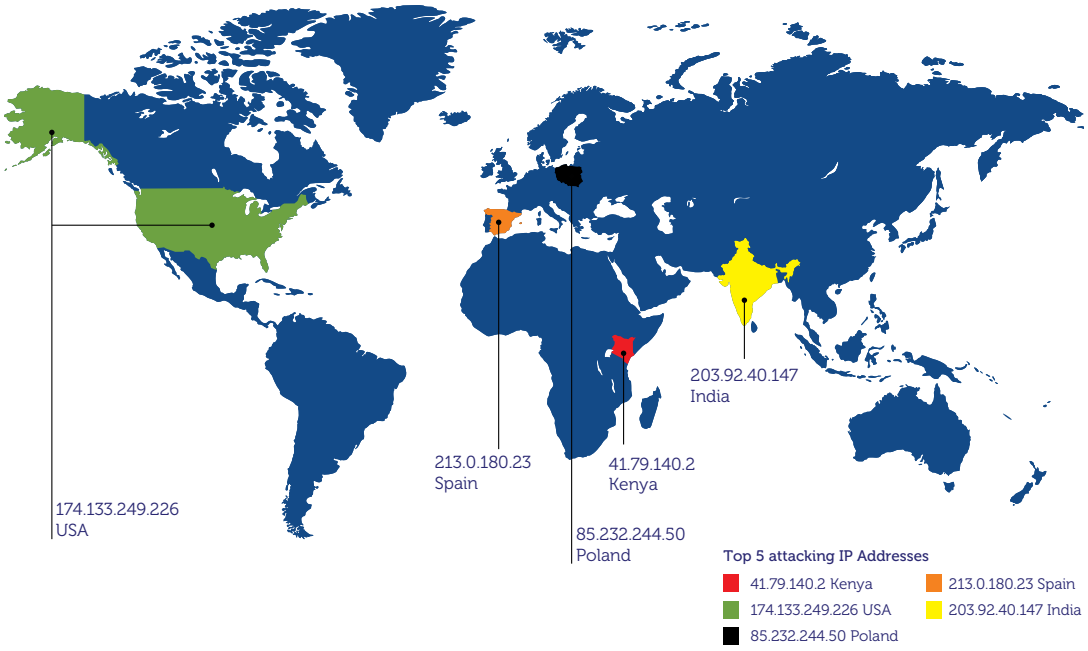
Malicious Kenyan IPs		
IP Address	ASN	Country
41.79.140.2	AS37396	Kenya
212.49.95.138	AS12455	Kenya
41.89.237.8	AS36914	Kenya
41.215.37.102	AS15808	Kenya
41.206.45.78	AS15808	Kenya
41.139.130.226	AS37061	Kenya
41.222.14.138	AS36866	Kenya
41.89.162.15	AS36914	Kenya
41.207.65.65	AS36915	Kenya
212.49.74.161	AS12455	Kenya
41.220.127.206	AS15808	Kenya
41.80.3.15	AS33771	Kenya
41.206.58.118	AS15808	Kenya
41.206.33.126	AS15808	Kenya
212.49.74.130	AS12455	Kenya

cont >>>

Top Attacking IP Addresses

IP Address	Country
178.162.205.226	Germany
62.75.236.82	Germany
41.79.140.2	Kenya
114.255.205.132	China
174.133.249.226	USA
85.232.244.50	Poland
213.0.180.23	Spain
203.92.40.147	India
61.160.200.74	China
200.214.185.34	Brazil

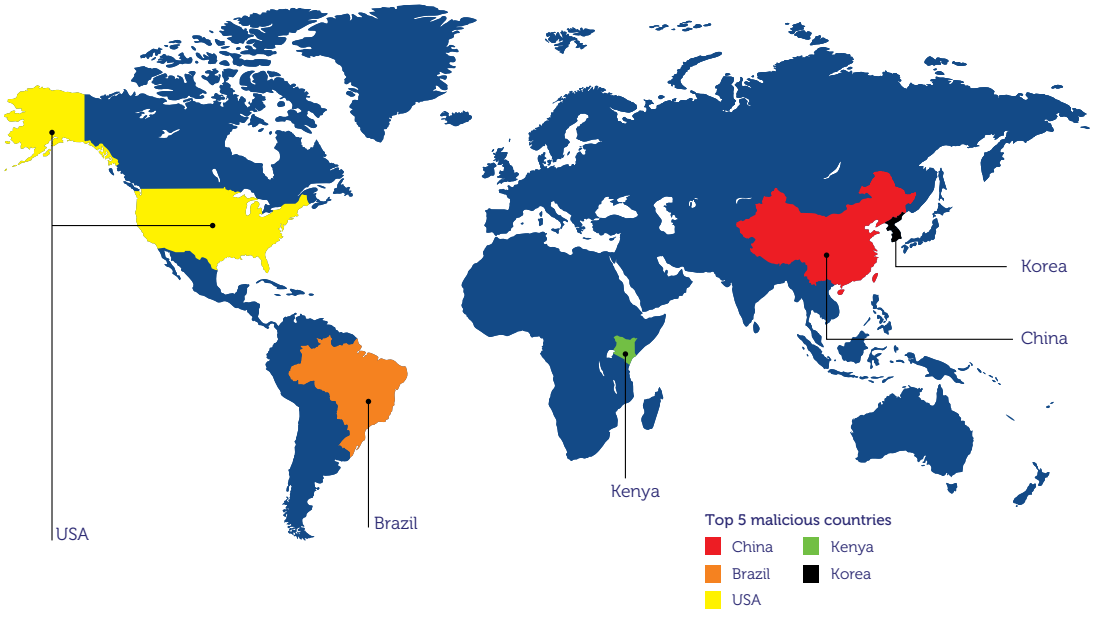
Table 3(c): Top Attacking IP Addresses



Map 1: Top Attacking IPs

Based on our statistics, the top attacking IP addresses are from Germany and Kenya. Malicious activity within the country has been on the rise over the period under review.

Top Malicious Countries



Map 2: Top malicious countries

The top 3 malicious countries are China, Brazil and the United States. China comes in first responsible for about a third of the total malware sent to the country.

Network Port Attacks

Port No	Service	Description
22	Secure Shell (SSH)/ Secure Copy (SCP)	This port is used for secure logins, file transfers (SCP, sftp) and port forwarding
3306	MySQL	MySQL Server port used for remote connections to the database
1433	Microsoft SQL	Microsoft SQL Server port used for remote connections to the database
3389	Terminal Server (RDP)	Remote Desktop Protocol(RDP) allows a user to connect to a remote computer running Microsoft Terminal services (also known as Remote Desktop Services). This is a mode of thin-client computing, where windows applications or an entire desktop is made accessible to a remote machine.
3128	HTTP-Proxy	Alternative port to 8080 that is also used for Web Proxy and caching server.
4899	Radmin	
80	HTTP	This port is commonly used by the server to listen to or expect to receive from a web client, assuming that the default was taken when the server was configured or setup.
8080	HTTP-Proxy	Commonly used for Web Proxy and caching server, or running web server as a non-root user.
23	Telnet	Telnet is a network protocol used on the internet or local area networks to provide a bidirectional interactive text-orientedd commnications facility using a virtual terminal connection.
25	SMTP	Simple Mail Transfer Protocol (SMTP) is used for e-mail routing between mail servers
5900	VNC Server	Virtual Network Computing (VNC) i.e. remote desktop protocol
445	Microsoft-DS	Microsoft-DS Active Directory, Windows shares
111	ONC RPC (Sun RPC)	ONC RPC (Sun RPC)
135	Microsoft EPMAP	DCE endpoint resolution
139	NetBIOS	NetBIOS Session Service provides services related to the session layer of the OSI model allowing applications on separate computers to communicate over a local area network.
443	HTTPS	Hypertext Transfer Protocol over TLS/SSL (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet

Table 4: Network ports description

Top Scanned Ports

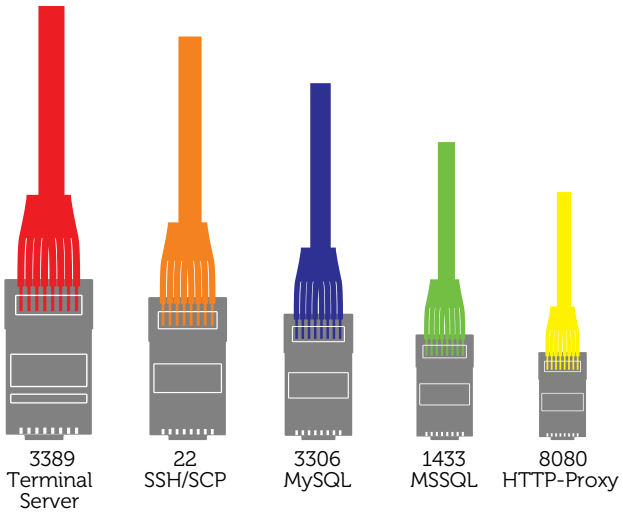


Illustration 1: Top scanned ports

Statistics of top scanned ports provide great insight in anticipation of future attacks. Most of the time, attackers would scan a network for open services in preparation for an impending attack. The illustration on the left highlights the top scanned ports in 2013 with port 3389, port 22 and port 3306 being the most scanned ports.

Top Attacked ports

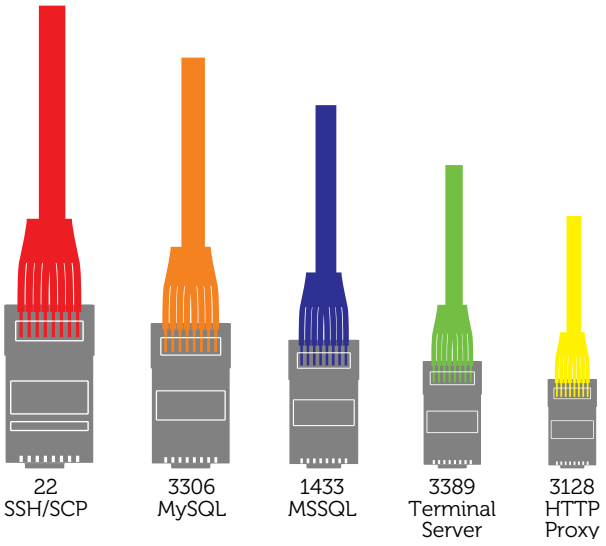


Illustration 2: Top attacked ports

The top attacked ports are port 22, port 3306 and port 1433. Port 22 and Port 3306 featured in the top 3 scanned ports and they have resulted in the top two attacked ports. It is interesting to note that half of the most scanned ports above resulted into actualized port attacks as shown in illustration 2.

B. Malware Threats: Viruses, Trojans and Worms, Botnets

Malware name	Malware type	Event count
Pushdo	Trojan	90.54%
Kelihos	Trojan	8.60%
Virut	Worm	0.61%
Nachi	Worm	0.24%

Table 5: Top Malware

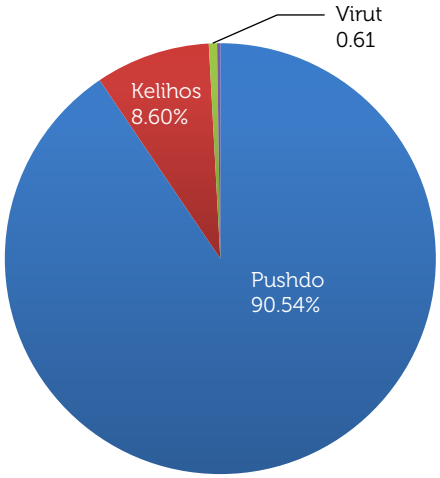


Chart 8: Top malware

The top malware in the country is the Pushdo Trojan that takes up about 90% of the top malware observed throughout the year.

Botnet Variants in Kenya

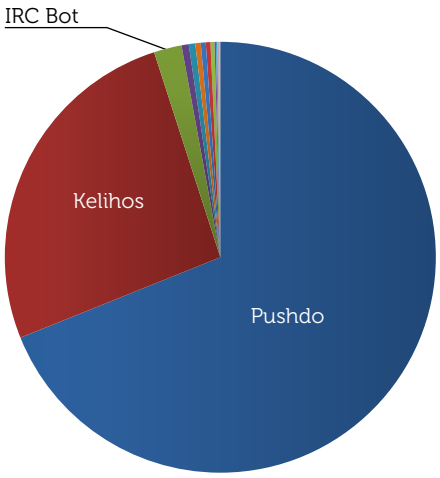


Chart 9: Top Botnets in Kenya

Botnets in Kenya are very rampant despite continuous international efforts in sink-holing activities. The top three variants are Pushdo, Kelihos and IRC bot.

1.3 Internet Service Providers: ISPs in Kenya

ISPs play a major role in the Kenyan Cyber space. They provide the key service of rolling out internet connectivity to the customers. ISPs stand at a very opportune position with respect to cyber security due to their unique role. They have the capability to track all malicious activity going in and out of their network and take necessary action. If ISPs were to co-operate in creating a clean cyber space in Kenya, there would be a significant change in the Cyber-attack landscape.

Top Malware Hosting ISP

ISP	Percentage
ISP 1	20.51%
ISP 2	17.75%
ISP 3	16.92%
ISP 5	16.74%
ISP 4	15.03%
ISP 10	4.17%
ISP 6	2.18%
ISP 8	1.30%
ISP 12	1.20%
ISP 7	1.05%
ISP 9	0.90%
ISP 14	0.52%
ISP 21	0.50%
ISP 11	0.49%
ISP 13	0.25%
ISP 18	0.23%
ISP 15	0.12%
ISP 19	0.07%
ISP 17	0.03%
ISP 16	0.02%
ISP 20	0.02%

Table 6: Top malware hosting ISP

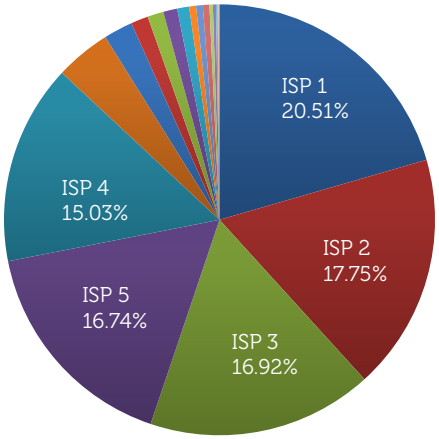


Chart 10: Top malware hosting ISP

The chart above highlights the Top malware hosting ISP. They are ISP 1, 2, 3, 5 and 4. Malware in ISPs is attributed to massive botnet traffic in and out of the ISP network.

Bot Activity per ISP

ISP	Percentage
ISP 3	18.93%
ISP 2	18.81%
ISP 1	18.45%
ISP 5	13.21%
ISP 14	10.93%
ISP 10	6.27%
ISP 4	6.22%
ISP 19	3.88%
ISP 9	1.03%
ISP 8	0.65%
ISP 6	0.33%
ISP 21	0.27%
ISP 11	0.23%
ISP 7	0.17%
ISP 18	0.17%
ISP 13	0.17%

Table 7: Bot activity per ISP

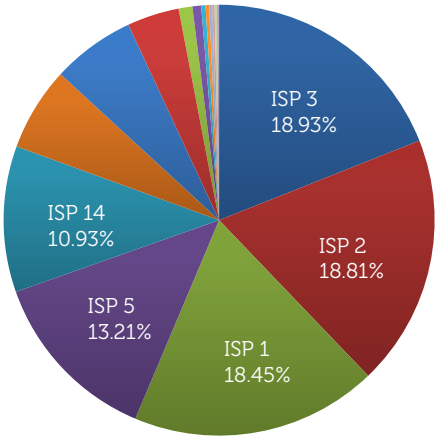


Chart 11: Bot activity per ISP

Botnets are a major concern in Kenya. The top four ISPs with large amounts of botnet traffic include ISP 3, 2, 1 and 5.

Spamming Activity per ISP

ISP	Percentage
ISP 5	68.13%
ISP 10	8.21%
ISP 2	7.55%
ISP 1	5.09%
ISP 19	3.85%
ISP 4	3.65%
ISP 14	1.43%
ISP 3	0.76%
ISP 8	0.22%
ISP 6	0.22%
ISP 7	0.19%
ISP 18	0.19%

Table 8: Spamming activity per ISP

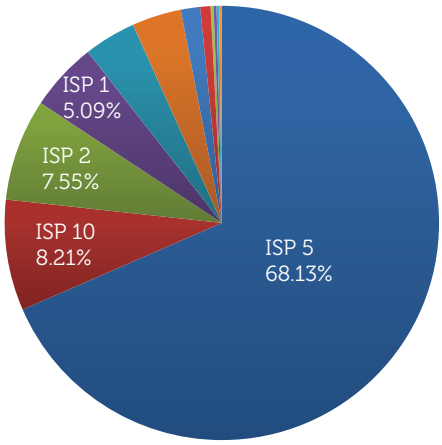


Chart 12: Spamming activity per ISP

It is interesting to note that a vast majority of spamming activity is specifically via ISP 5. This may be atributed to poor spam filtering mechanisms implemted by the ISP.

DNS Attacks per ISP

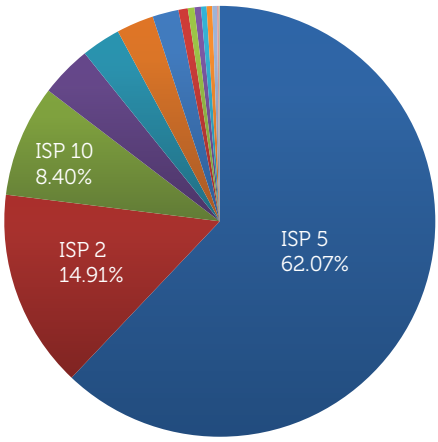


Chart 13: DNS Activity per ISP

ISP 5 has the most DNS server attack activity eminating from its servers. DNS attacks are quickly becoming more prevalent due to the large number of open resolvers that are poorly configured.

Top Proxy Attacks per ISP

ISP	Percentage
ISP 12	48.06%
ISP 4	20.30%
ISP 1	11.81%
ISP 19	10.85%
ISP 2	7.33%
ISP 10	1.37%
ISP 3	0.16%
ISP 5	0.11%
ISP 6	0.01%

Table 9: Top Proxy attacks per ISP

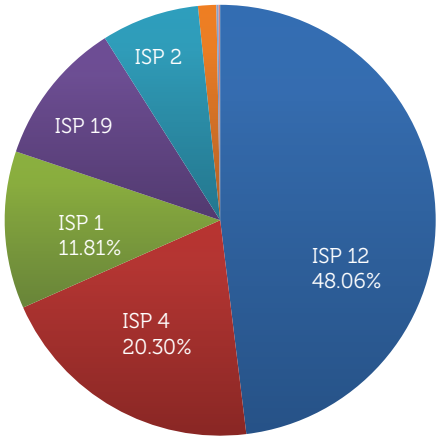


Chart 14: Top Proxy attacks per ISP

Proxy server attacks are only featured in a few ISPs. The top ISPs with a majority of malicious proxy traffic include ISP 12, ISP 4 and ISP 1.

1.4 Threat Activity Trends

Quarter	Proxy	Trojan	Botnet	PBX Attack	Malware
Q 1 2013	50000	130000	200000	120000	300000
Q2 2013	60000	150000	400000	160000	400000
Q3 2013	80000	200000	500000	200000	450000
Q4 2013	100000	300000	700000	300000	600000

Table 10: Trend Analysis per Quarter

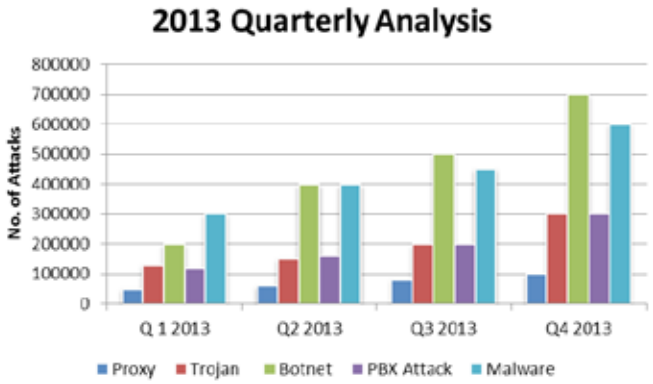


Chart 15: Trend Analysis per Quarter

Year	PBX Attack	Malware	Botnet	Proxy	Trojan
2012	450000	1000000	900000	50000	200000
2013	780000	1750000	1800000	290000	780000
% increase	73%	75%	100%	480%	290%

Table 11: Trend Analysis 2012 vs 2013

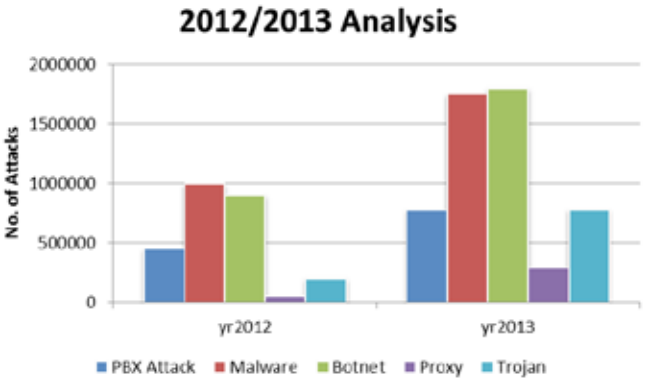


Chart 16: Trend Analysis 2012 vs 2013

Vulnerabilities and Exploits: 2012 vs 2013

The statistics in this section are courtesy of **www.cvedetails.com.** They are a comparison of two years i.e. 2012 and 2013. The significance of this data is to highlight the changes in vulnerabilities and exploits observed in this given duration. We also highlight vendors and products with their respective vulnerabilities.

Vendor Vulnerabilities

	Year	
Vulnerability Type	**2012**	**2013**
DoS	1425	1453
Code Execution	1455	1184
Overflow	844	859
Memory Corruption	423	366
Sql Injection	242	155
XSS	757	650
Directory Traversal	122	109
Http Response Splitting	13	7
Bypass something	343	349
Gain Information	389	510
Gain Privileges	250	274
CSRF	166	123
File Inclusion	14	1
Total	8455	8053

Table 11: Vendor vulnerabilities

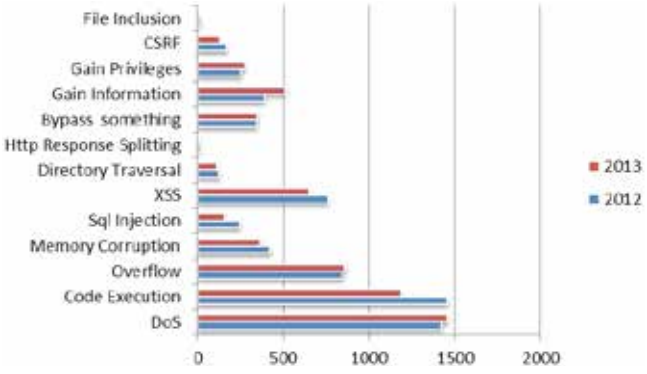


Chart 17: Vendor vulnerabilities

The top three vulnerabilities for the year 2013 were DoS, Code execution and overflow in contrast to the year 2012 where code execution was leading, closely followed by DoS and Overflow.

This shows that the threat landscape is dynamic and highly volatile. While vendors increased controls to mitigate DoS, cyber criminals quickly adapted and shifted to utilizing code execution.

Vulnerabilities vs Exploits

	Year		% Change
Vulnerabilities and Exploits	**2012**	**2013**	**% Decrease**
No. of Vulnerabilities	5295	5191	1.96%
No. of exploits	611	185	69.72%

Table 12: Vendor vulnerabilities vs Exploits

Exploits are tailored to take advantage of vulnerabilities hence their co-existence is quite inevitable. The number of vulnerabilities identified in 2013 declined by 1.96% from 5,295 reported in 2012 to 5191 in 2013.

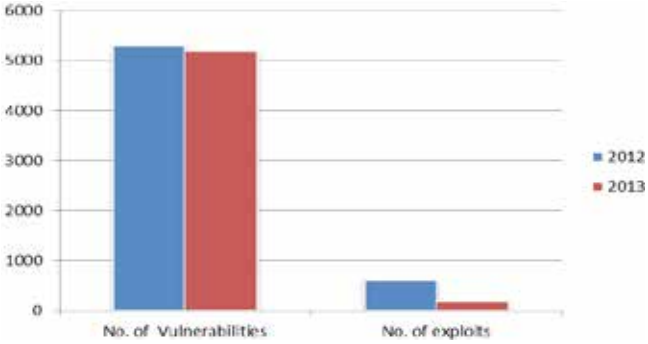


Chart 18: Vulnerabilities vs Exploits

The numbers of exploits developed in 2013 are less compared to 2012. The number of exploits reported in 2013 was 185 compared to 611 exploits reported in 2012. This sharp decline is due to efforts by both government and state agencies to curb cyber-crime at an international level with the arrest of several cyber-criminal group members.

Top 15 Vendors by Total Number of "Distinct" Vulnerabilities, 2013

2012		2013	
Vendor Name	No. of Vulnerabilities	Vendor Name	No. of Vulnerabilities
Oracle	380	Oracle	496
Apple	309	Cisco	433
Google	278	IBM	394
Mozilla	203	Microsoft	345
IBM	175	Google	192
Microsoft	172	Apple	192
Cisco	160	Redhat	191
Adobe	146	Linux	190
Linux	116	SUN	175
SUN	99	Mozilla	160
Moodle	95	Adobe	148
HP	84	HP	144
Apache	63	Novell	91
Mysql	59	Wireshark	82
Ffmpeg	54	Ffmpeg	77
Total	2393	Total	3310

Table 13: Top 15 Vendor vulnerabilities

The vendor vulnerabilities have shifted considerably in the year to year comparison. The top 5 vendors with vulnerabilities in 2012 were not replaced by other respective vendors in 2013. Only apple and Mozilla reported lower numbers of vulnerabilities. This shows some effort by vendors to reduce the number of vulnerabilities in their products. It is interesting to note that Microsoft, IBM, Oracle and Cisco had a higher number of vulnerabities reported in 2013 as opposed to 2012 with Cisco reporting the highest increase in vulnerabiities.

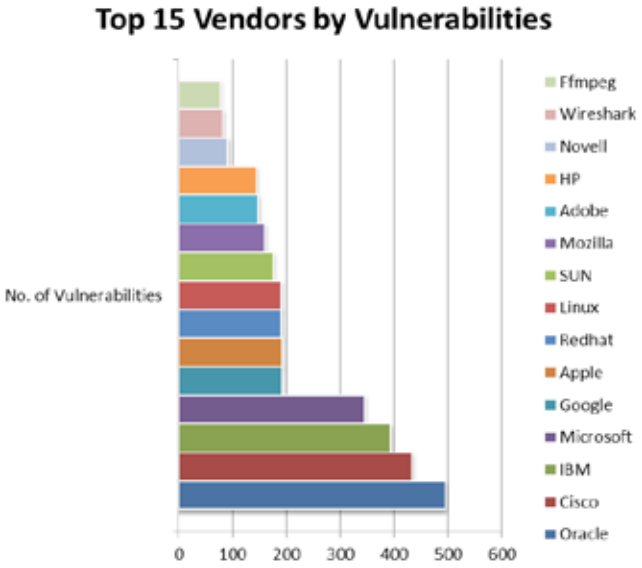


Chart 19: Top 15 vendors by vulnerabilities 2013

The top 3 vendors with the most vulnerabilities were Oracle, Cisco and IBM. Oracle had 496 vulnerabilities across its products, followed by Cisco with 433 and IBM with 394 reported vulnerabilities.

Kenya Cyber Security Report 2014

Top 15 Products By Total Number of "Distinct" Vulnerabilities, 2013

2012				2013			
Product Name	**Vendor Name**	**Product Type**	**No. of Vulnerabilities**	**Product Name**	**Vendor Name**	**Product Type**	**No. of Vulnerabilities**
Chrome	Google	Application	249	Linux Kernel	Linux	OS	190
Firefox	Mozilla	Application	162	JRE	Oracle	Application	180
Thunderbird	Mozilla	Application	147	JDK	Oracle	Application	180
Seamonkey	Mozilla	Application	146	Chrome	Google	Application	175
Firefox Esr	Mozilla	Application	115	Firefox	Mozilla	Application	149
Linux Kernel	Linux	OS	115	JDK	SUN	Application	131
Iphone Os	Apple	OS	112	JRE	SUN	Application	131
Itunes	Apple	Application	111	Internet Explorer	Microsoft	Application	129
Thunderbird Esr	Mozilla	Application	109	Thunderbird	Mozilla	Application	113
Moodle	Moodle	Application	95	Windows Server 2008	Microsoft	OS	104
Safari	Apple	Application	88	Seamonkey	Mozilla	Application	104
Flash Player	Adobe	Application	66	Windows 7	Microsoft	OS	100
Mysql	Oracle	Application	65	Firefox Esr	Mozilla	Application	100
Fusion Middleware	Oracle	Application	64	Windows Vista	Microsoft	OS	96
Mysql	Mysql	Application	59	iphone OS	Apple	OS	90
Total			**1703**	**Total**			**1972**

Table 14: Product vulnerabilities

The Top 5 products with the most vulnerabilities reported are Linux kernel, JRE, JDK, Chrome and Firefox. Linux has 190 vulnerabilities, JRE and JDK tied at 180, chrome at 175 and Firefox at 149. Across the board 2015 had a higher number of product vulnerabiities reported of 1972 as opposed to 2012 where only 1703 were reported.

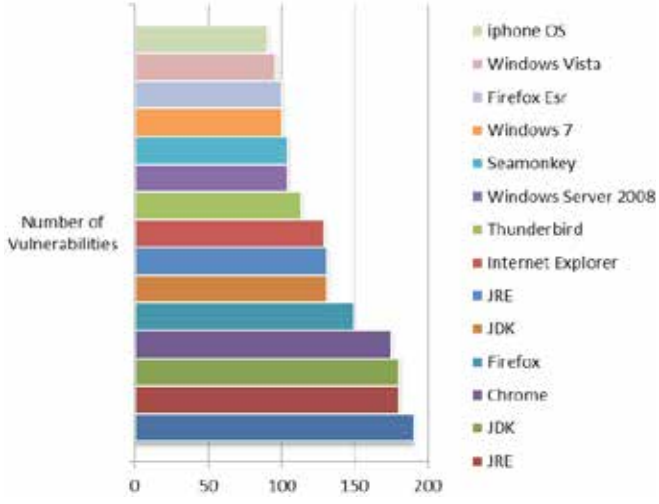


Chart 20: Top 15 products by vulnerabilities

45-DAY FREE TRIAL & DISCOUNT ON
SERIANU LOG MONITORING & ANALYSIS SERVICE

The Package includes FREE maintenance, support and security assessment services to help customers in East Africa correlate system and network events through rules, reports and dashboards.

LOG MONITORING AS A MANAGED SERVICE

Automatically collect, analyze and monitor system logs for auditing needs and to identify user violations & unauthorized activity.

Key Features, Benefits and Functionality

- Monitor all administrator activities – including activities initiated by super users.
- Archive events on a long-term basis for auditing requirements.
- Automatically generate reports and alerts via email and SMS to security officers.
- Track database changes - Insert, Update, and Delete Operations.
- Produce detailed system data access and network user activity report.
- Monitor remote users accessing the network via VPN and secure channels.

Service Brief

Serianu has partnered with AccelOps, a leading information security service provider to develop The Serianu Log Threat Monitoring & Analysis Service, a customized security monitoring solution for the East African region. This solution incorporates local cyber threat intelligence – including a list of potentially malicious IP addresses including malware hosts, spam sources and other threats.

Limited Time Exclusive Promotion

We are currently offering a Limited Time Exclusive Promotion for The Serianu Log Threat Monitoring & Analysis Service that includes a **45-Day FREE TRIAL/PROOF OF CONCEPT** Deployment, discounted pricing and one year of **FREE** maintenance and support for customers in East Africa. The package includes **FREE** security assessment services to help customers correlate system vulnerabilities with event and network data, helping to prioritize security incidents through rules, reports and dashboards.

SERIANU

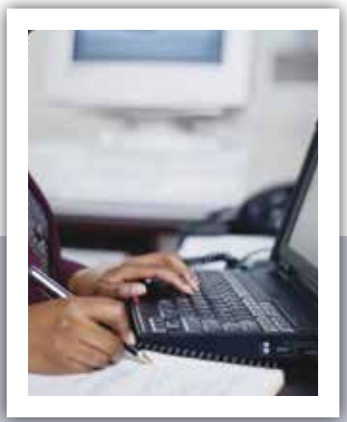
accelops

Tel: +254 710 241 892 or +254 702 847 570 | info@serianu.com | www.serianu.com

SERIANU

SIEM OPTIMISATION & LOG MANAGEMENT

Gain Actionable Insights, Monitor Enterprise Activity and Manage Risk



Our service will enable you to:

- Detect and prevent security breaches.
- Conduct forensic investigations on security incidents.
- Automate the entire log management process.
- Comply and prove compliance.
- Automate routine tasks and decrease dependence on existing resources.
- Accelerate troubleshooting times.
- Free up personnel to do more productive tasks.
- Leverage market leading Accelops Technology.

Background

Despite the obvious benefits of Log Management and its increasing recognition as a critical necessity by most organizations, Log Management is still viewed by businesses as a tactical and manual effort. In a typical organisation, millions of logs are generated by systems, applications and devices every single day. These logs contain a record of all activity that takes place in a network and provide a wellspring of information to help improve security, enable compliance and optimize IT operations.

The SIEM Optimisation & Log Management

The Serianu service provides a robust log collection, alerting and archival solution that is designed to be an important component of your organization's risk management strategy, providing you with valuable tools to help your organization address its applicable compliance requirements.

Historically, enterprise-class log management solutions have been extremely expensive and time-consuming to implement. However, our service provides all of the functionality of an enterprise-class solution, without the significant up-front costs and implementation time lines. This allows you to focus IT staff on tasks that help drive revenue and provide differentiation for your organization, rather than focusing on routine log management activities.

Our Approach

Gaining any actionable intelligence from this data, however, depends on how well you can collect, consolidate, store and decipher the information that event logs contain. Our approach provides you with an integrated set of tools and services that can easily fit into your existing environment, enabling you to collect, store, analyze and archive your logs.

Comprehensive Deployment and Configuration Services

Since the Log Management Service is a managed service, you can rely on Serianu to:

- Provide the log collection appliance and work with your

organization to set up and configure the service.

- Work with your organization to determine your logging rate, measured in messages per second, and also determine the appropriate size of the service - offering to deploy. Serianu can also be engaged in helping you pre-determine your anticipated logging rate.
- Provide you with log source configuration guidelines for supported devices, for later use by your device administrator.

Log Collection

The service supports a wide variety of security and network devices, Operating Systems, and applications. (A full list of supported devices is available upon request). Logs are collected via a dedicated collection appliance, and then transmitted, to redundant storage and reporting infrastructure.

Reporting and Alerting

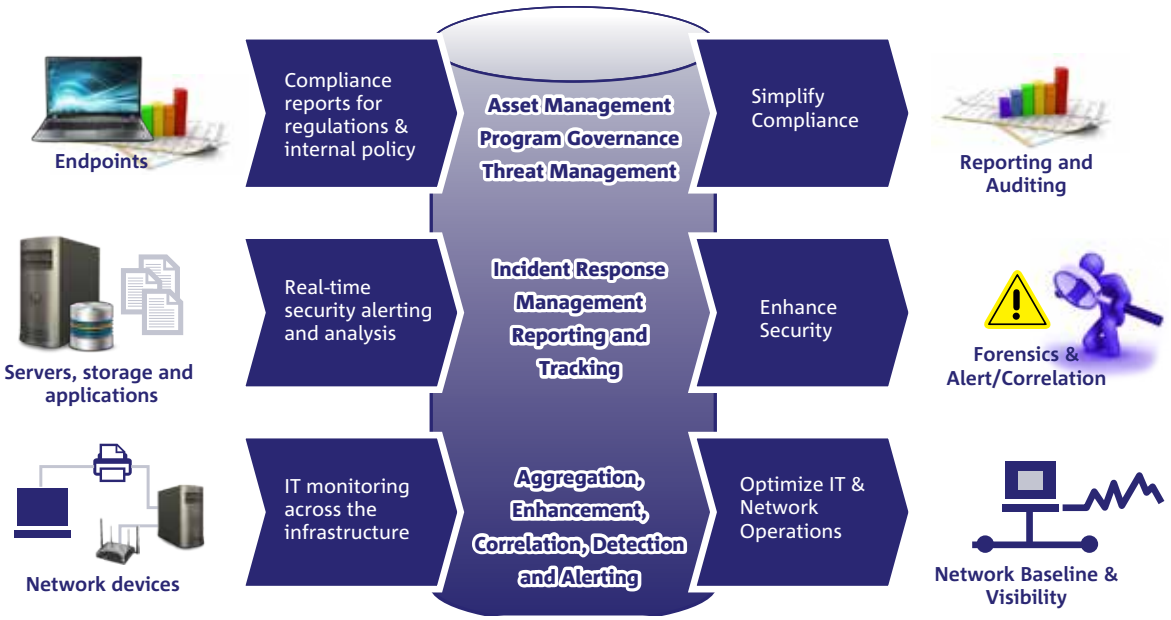
The service includes a standardized set of reports, including those related to specific security standards. In addition, Serianu provides you with access to the logging appliance to run customizable reports, guidance regarding how you can utilize the reporting interface and how to create customized reports.

With the service, you receive alerting based on standardized, pre-defined alert criteria, with up to twenty customized alert-rules also available.

Storage and Archival

Serianu will work with you to deploy a high-availability storage infrastructure, with daily back-ups to support the service. For your further protection, we can enable your infrastructure to runs ongoing integrity checks to verify that log data has not been altered.

Although log management solutions are typically deployed to meet very specific requirements, they have benefits that extend far beyond department level objectives. The Serianu service will automate the collection, consolidation and analysis of log data, benefiting a growing number of constituents within your organisation. These groups range from audit and compliance security teams, IT operations, help desk teams, legal teams (for forensic investigation) to senior management and CIO's.



The Serianu Log Management Service Diagram.

SERIANU

Section 2: Enterprise Security

From our analysis, security at the enterprise level is still in its infancy in Kenya. This however is rapidly changing, as enterprises begin to gain an understanding and appreciation for the value of security in their organisations. This has been influenced by the rate at which organisations have been attacked recently as well as pressure from the Kenya cyber security community advocating for better security at the enterprise level.

A majority of local organisations rely heavily on applications and systems to provide services both internally to the organisation or externally to their consumers. Such applications often store, process or transport sensitive data. They are also connected to the core and critical infrastructure of the organization. With this in mind, such assets are usually targeted due to the high value data they interact with. This section takes a look at the applications and systems targeted by malicious individuals and the vulnerabilities they exploit. This is of great value in understanding the gaps present in applications and systems we use on a day to day basis.

2.1 Web Applications

2.1.1 Online Banking

Online banking allows customers of a financial institution to conduct financial transactions on a secured website operated by the institution. To access online banking a user must be registered with the institution for the service and have a password for customer verification. Attacks on online banking are based on deceiving the user and stealing login data through Phishing, malware, Cross-site scripting, Keyloggers/ Trojan horses and pharming.

In February 2014, we conducted an independent review of online banking; shopping and payments websites in Kenya. The study revealed that Kenyan online banking portals have limited security mechanism to protect the customer's login credentials to the platform. Out of 33 banks sampled, only 2 banks had client side encryption implemented. This means that for the remainder of the banks, a sniffer on a customer or end user PC network will reveal the user's password in plain text. Akeylogger on the customer's PC would capture all passwords and key strokes even for secured https sites. It should also be noted that the SSL encryption used on the various bank sites are not well implemented, meaning that they can be easily circumvented in order to perform man-in-the-middle attacks.

2.1.2 Online Shopping

Online shopping refers to the ability to buying goods or services from a seller over the internet. The increase in online transactions has led to an increase in the number and type of attacks against the security of online payment systems'. Vulnerabilities that affect these systems include SQL injections, cross-site scripting andbuffer overflows. Methods used to attack online shopping websites are: Botnet, and DoS attacks, Fraud, Phishing scams that lead to cybercriminals obtaining user passwords and names.

In February 2014, we conducted a study of the top Online Payment and shopping Sites in Kenya. We discovered that all of the top four Online Payment Sites have no client side encryption security mechanisms in place. The growing number of online shoppers is exposed to the risk of getting their sensitive information leaked. This means that the credentials used to access the websites, if intercepted; can be viewed in plain text.

2.2 VOIP PBX Fraud

Voice over Internet Protocol (VoIP) networks allow people to make phone calls over the Internet at very low or no cost at all. VoIP is affordable, but it still lacks proper security features. In a VoIP setup, your handset is often a computer connecting to the Internet. It communicates with a VoIP server and uses a username and password. Once authenticated it can make calls over the Internet. However, if those calls exit the VoIP Server upstream to access the destination of the call then that VoIP Server is going to be billed for the call.

2.2.1 What is VoIP Hacking?

VoIP hacking is the use of tools and scripts to crack the password of the respective SIP accounts on a VoIP system so as to facilitate making free phone calls, eavesdropping on

conversations, changing caller IDs, disrupting phone calls and accessing sensitive information. Generally the hacker would be looking to get the account registration details and the password to authenticate to a VoIP server so that they can register a SIP client and make calls.

In the event malicious attackers have an individual's VoIP account details, they can make calls for free, thus saving them money. In the case of organized crime seeking higher returns, accounts are used to make thousands of calls.

- **Why it Happens?** VoIP is readily being targeted for fraud because the VoIP industry has grown substantially and is now a major player in the telecommunications domain. Therefore cybercriminals will always be targeting PBX systems to exploit them to their own benefit. Due to the lax international communications standards and regulation in Kenya, it is relatively easy to exploit such services without much of a consequence or ready detection. This is because VoIP hacking does not require much specialized equipment and there is little barrier to entry for a potential scammer.Cyber criminals are also aware of the fact that there is little to no security oversight for many VoIP customers. A majority of the Kenyan corporates never even realize that they have been the victims of VoIP fraud until they see the bills. Few enterprises have proactive detection mechanisms and controls in place to mitigate this type of attack.

- **Current security threats on VoIP services:** The primary threat is that cybercriminals gain access to your SIP account (your VoIP telephone) line by cracking your password and then make calls to destination where they get a share of the cost of the call.

The immediate implications for businesses attempting to rollout VoIP within their business are:

- Businesses must make sure that they understand the threats and the measures they can take to minimize the risks.

- They must institute policies for the password staff use with their VoIP accounts, very strong computer generated passwords should be used.

- Firewall policies must be updated to cater for the VoIP protocols.

- Defense in depth is a useful guideline. Do not rely on only one type of protection for any part of the system. For example, don't just use good passwords, but also restrict access by IP address if possible.

- Consider the credit control of how much you deposit in your VoIP account if it is pre-paid or set a limit for only the level of calls you usually make if the account is postpaid.

Average cost implications for a VoIP recovery process

- If the credit limits are not set on your VoIP account then the cost implication could be severe and can run into several Millions of shillings. The cost would tend to increase the longer the attack goes undetected and remediated.

The VoIP Provider

- If cyber-criminals gain access to the VoIP provider's servers, they could route many calls via the company's VoIP server running up bills, make free calls or lease VoIP services at a fee at the expense of the compromised provider.

- Cyber criminals make money from the end consumer, who paid to use 'their network', but was instead channeled through a 'free path' at no cost to the criminal. Those placing phone calls were unlikely to have any idea that their calls went through this system to their destination.

The Enterprise

- In Kenya, our there have been several VoIP attacks detected by our sensors and it came to light that several organizations had their VoIP server hacked last year. The affected organizations only realized that their VoIP servers were hacked into after being served with a bill running up to several million Kenya shillings. The mentioned organizations inevitably had to settle the bills with their VoIP carrier.

What Can I Do If I am Hacked?

- In the event you VoIP server is hacked there is very little that can be done to revert the financial damage. Your VoIP provider will still require you to pay the respective bills. The next step should be to secure your VoIP infrastructure form future attacks.

2.2.2 Recommendation

Ensure your VoIP provider has anomaly detection systems in place to notice if your spend goes up dramatically in a short period of time.

VoIP hacking takes advantage of poor or non-existent security measures on SIP infrastructure. If no security measures are taken then your servers are exposed to attacks. VoIP hacking is different from web application hacking in the sense that once your server has been compromised, cybercriminals will bleed money right out of your organization in a matter of hours.

2.3 Insider Threats

2.3.1 Insider Attacks in Kenyan organisations getting deadlier

Our research reveals that the insider threat landscape in many Kenyan organisations is becoming more complex with multiple risks that are currently being managed by multiple point technologies. Internal security risks represent a wide range of deliberate and accidental incidents. The scope of the problem only intensifies as business models continue to evolve with increased mobility, a growing mix of users, and geographically diverse business offices.

Insider threats in Kenya contain a high incidence of deliberate malicious activity by current employees. Privileged users probe systems for unauthorized access, co-opt other user's access privileges, and attack systems for a variety of reasons including disgruntlement, revenge, competitive advantage and blackmail. The fact that most of these users are employees and their system access is authorised makes detection difficult.The risk posed by the high percentage of employees with laptops, mobile phones, PDAs, multiple email accounts, and access to applications and databases makes addressing the insider threat a substantial challenge. Reducing the vulnerabilities posed by internal users needs to be a key priority in Kenyan organisations' security strategies.

Kenyan organisations need to look at holistic solutions which include controlling access rights, reviewing activity, analysing anomalous behaviours, monitoring inbound and outbound traffic for confidentiality violations, and encrypting data. In both cases (accidental and deliberate), the goals should be the same: prevent most incidents, respond quickly and accurately to any problems, run forensics after incidents, and feed the results back into the prevention mechanisms.

Publicly reported cases of insider threat in 2013

- In 2013, Banking Fraud Investigations Department (BFID) reported that Ksh1.49 billion ($17.52 million) was stolen from customers' accounts between April 2012 and April 2013 through schemes hatched by employees. Unfortunately, fraud is on the rise as cashless transactions continue to become more popular – internet banking, mobile money transfers, RTGS, credit card, and cheque payments.

- A leading telecommunications service provider sacked 33 employees over cases of economic crime, including accounting fraud and asset misappropriation.

- A leading commercial bank employee was charged with defrauding the bank of Sh60 million.

2.4 Industry Trends

2.4.1 SIEM (Security Information and Event Management Tools) Adoption

As threats become more severe and complex, the demand for security information and event management tools in Kenya is growing. In the past one year, we have noted that local organizations are taking a closer look at products that incorporate multiple functions -- such as logging, reporting, network behavior analysis and alerts -- in an appliance or enterprise software. While SIEM deployment is a great initiative, it is important for organizations to understand the challenges that come with these deployments.

SIEM deployment projects should be treated as enterprise wide projects that require the participation of different departments in the company including: ICT, Security, Risk management, Compliance and Human resources. The following factors should be considered before embarking on a SIEM/Log management project:

- The organization should fully understand internal incident response and logging requirements
- Define and develop a suitable SIEM/Log management service delivery model – even before deploying the SIEM solution (technology tool).
- Plan and develop a clearly defined SIEM/log management strategy (e.g. for compliance (PCI DSS) and threat management (cyber threats)
- Gather requirements from key stakeholders including Risk, compliance, ICT, Security, business units etc.
- Develop analytics and workflow requirements to ensure all critical incidents are captured and responded to in a timely manner
- The organisation should have an updated and accurate Information asset register
- Develop an information security governance framework
- It is important to note that without considering these factors, the SIEM/Log management technology solution will not effectively fulfil its intended purpose.

2.4.2 WAF (Web Application Firewall) Adoption

The explosion of mobile devices has facilitated the migration of business processes to the Internet, making enterprises wary of the threats and risks in cyberspace. Kenyan organisations, therefore, are turning to Web application firewalls (WAF) to meet their security needs. The increasing sophistication of cyber threats targeting Web applications has further compelled businesses in the region to adopt WAF solutions. In the banking sector, almost all the banks are introducing internet banking which requires firewall protection.

2.5 Employees are Bringing their Own Devices(BYOD)

With the continued adoption of enterprise mobility, a growing percentage of workers are using their personal devices to access corporate resources. When these devices are not secured, this introduces a wide range of security threats. Our research suggests that this trend is only increasing; many employees in Kenyan organizations are using their personal devices to access business applications and resources.

This trend is introducing new risks to the organizations, such as:

- Loss, disclosure or corruption of corporate data on employee owned devices;
- Incidents involving threats to or compromise of, the corporate ICT infrastructure and other information assets (e.g. malware infection or hacking);

- Noncompliance with applicable laws, regulations and obligations (e.g. privacy or piracy);
- Intellectual property rights for corporate information created, stored, processed or communicated on PODs in the course of work for the organization.

Rather than trying to mitigate this trend by further locking down corporate resources, corporations are taking advantage of it by empowering and securing the personal device for business use through Bring Your Own Device (BYOD) programs.

2.6 Credit & ATM Cards; Theft and Fraud

The total number of credit cards in circulation in Kenya for the year 2013 stood at over 10 million. In terms of transactions, this translates into movement of transactions worth billions every month. The presence of such large numbers of credit cards in the possession of a vast majority of unsuspecting bank account holders attracts fraudsters whose main target is to obtain your credit and ATM card information. Kenyan banks have lost millions over the year, due to the volatile combination of malicious tech-savvy employees and social engineering.

Skimming has become especially popular in Kenya over the past year. The rise in skimming and other card fraud/theft cases forced the Kenya Bankers Association (KBA) to set a June 2014 deadline by which all lenders should migrate to the chip-based technology for debit and credit cards. The more costly EMV (Europay MasterCard Visa) chip based cards are far less vulnerable than the legacy magnetic strip cards.

Skimming has become especially popular in Kenya over the past year. The rise in skimming and other card fraud/theft cases forced the Kenya Bankers Association (KBA) to set a June 2014 deadline by which all lenders should migrate to the chip-based technology for debit and credit cards. The more costly EMV (Europay MasterCard Visa) chip based cards are far less vulnerable than the legacy magnetic strip cards.

2.7 Content Management Systems

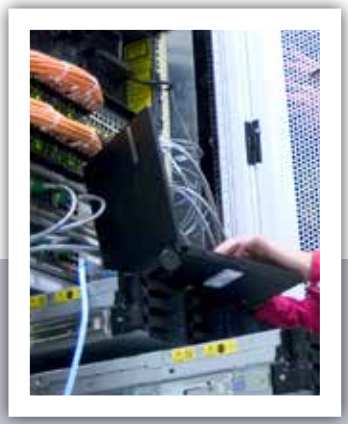
Joomla is a free content management platform that is used to publish web content. It is used to develop websites and online applications. Joomla is quite popular as it is freely available and easy to use. As like any other product, it has its fair share of vulnerabilities. Due to the popularity of this platform, it is heavily targeted hence vulnerabilities are discovered quite regularly.

In Kenya, joomla and wordpress are the most attacked platforms as they share similar characteristics in terms of the nature of the product. It is interesting to note that most organizations and individuals that deploy websites built on these platforms do not take the necessary measure to secure them. This leaves the websites ready for takeover by malicious attackers. Joomla and wordpress attacks are very rampant despite the respective vendors providing regular patches against vulnerabilities on their respective product.

SERIANU

INSIDER THREAT MITIGATION AND IDENTITY ASSURANCE SERVICE

Detecting and Protecting Against the Malicious Insider



Our service will enable you to:

- Get proactive about insider threats.
- Hold trusted users accountable.
- Investigate suspicious behaviour.
- Respond in real time to attempted fraud.
- Prevent the next crime.
- Comply with government and industry regulations.

Background

Recent information security studies have shown that approximately two thirds of fraud and identity-theft cases are being perpetrated by company employees and other insiders. This information combined with increased reports of fraud cases, is a clear indication that insiders are responsible for the vast majority of losses sustained by enterprises—whether from malicious abuse of information and IT or sidestepping procedural controls. Despite the tendency for enterprises to do little about insider abuses and focus on external attacks, many suitable techniques should be judiciously applied to protect against the malicious insider.

The Serianu Insider Threat Mitigation and Identity Assurance Service

The Serianu Insider Threat & Identity Assurance is a first-of-its-kind, integrated service for unparalleled visibility of insider threats activity with intelligent threat detection and prevention framework. The service has the capability to operate in real time (prevention) and / or in batch (detection) modes, and therefore supporting mitigation of threats in the following areas:

- **IT Sabotage** - A trusted user uses information technology (IT) to effect specific harm at an organisation or an individual.
- **Fraud** - An insider's use of IT for the unauthorized modification, addition, or deletion of an organisation's data for personal gain, or theft of information that leads to an identity crime (e.g., identity theft, credit card fraud)
- **Theft of Intellectual Property (IP)** - A trusted insider's use of IT to steal intellectual property from the organisations.
- **Accidental** - A trusted user's unintentional use of IT systems results in misuse, accidents, or other unintentional sources of risk to the organisation.

Our Approach

Our Insider Threat Mitigation service accelerates business innovation by formalizing organisation-wide strategies for minimizing fraud attempts, assuring, protecting, detecting, and managing user identities, sharing intelligence on the latest fraud trends and attacks, and establishing operational controls.

Discover the inherent insider threats

In this phase we focus on understanding your business and identifying any potential insider threats.

We work with you to:

- Conduct an assessment of your current efforts to mitigate insider threats
- Define an insider threat strategy for products/services, channels, and/or the organisations
- Develop a roadmap and business case for investments
- Gain the organisations consensus necessary to approve funds and initiate change

Implement the right controls to mitigate against insider threats

This is a follow up to the Insider Threat Risk Assessment and Strategy development phase and defines the proposed implementation approach for the Insider Threat Mitigation strategy implementation.

- Acceleration of effective policies and insider threat mitigation program
- Develop comprehensive security and insider threat awareness curriculum
- Define and establish appropriate controls for Insider Threat Mitigation
- Architect suitable mechanisms to Identity Assurance and Access Management

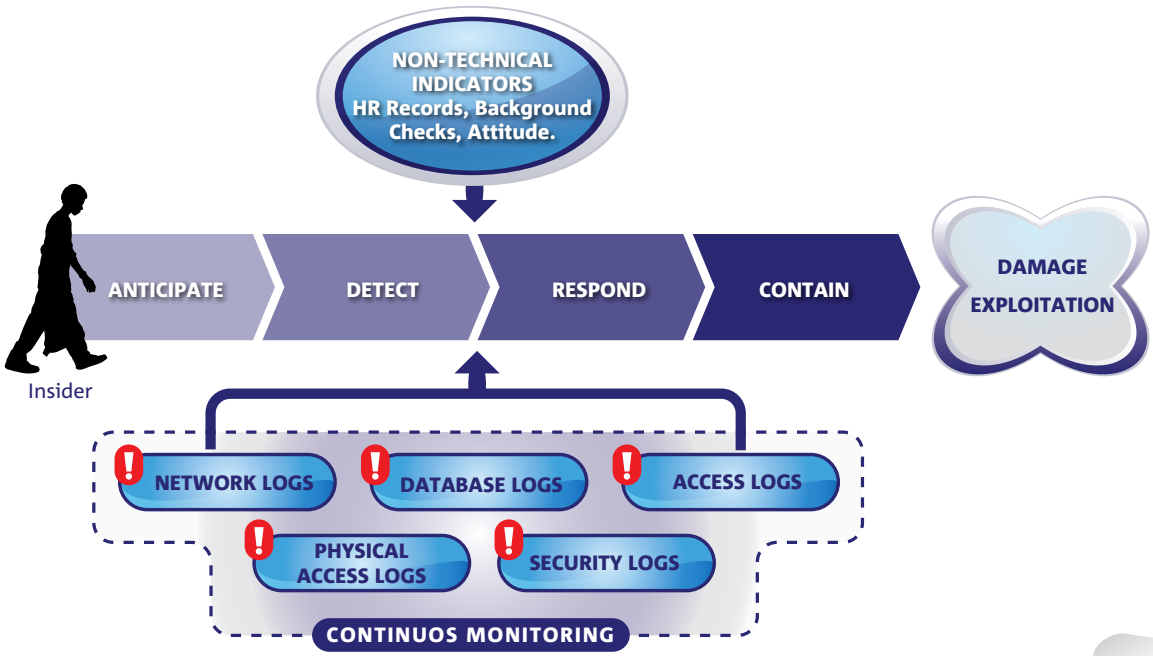
Continuously monitor and improve implemented controls

This phase focuses on building the capability to monitor insider threats on a continuous basis and transition from a reactive to a proactive approach. By utilizing near real-time monitoring techniques, you will be able to investigate and resolve issues that might otherwise go undetected. In addition to ensuring insider threats are detected in real-time, the solution provides the organisation with additional assurance around compliance relating to internal and external requirements.

- Continuous monitoring, detection and prevention
- Evaluate controls, modeling and tuning, and intelligence sharing
- Communicate policy, procedures, guidelines and essential insider threat awareness
- Adherence to policy, reporting of incidents and escalation as required

Conclusion

Many organisations view insider threats as a homogenous threat landscape; “Insiders (employees, vendor and contractors) with authorized access will do bad things and there will be a negative business impact. While this description is somewhat accurate, it doesn’t provide enough information with which to manage this risk.



Section 3: End user/Consumer Security

In the advent of increased cyber usage, the internet facilitates access to both products and services at the click of a button. We use the internet to shop online, perform banking transactions, and communicate with peers, share videos and documents; simply due to the interconnectivity of our devices.

Internet adoption in Kenya has greatly grown due to the demand for the infrastructure to facilitate business and improve service delivery to respective consumers. The rise of internet connectivity adoption in Kenya, translates into more users connecting to the internet. With the current trend, internet connectivity from the comfort of your home is now possible. With this resource, there are a few risks such as fraud and scams. This therefore means that more consumers are being exposed online as they carry on their day to day activities. It has become critical for every internet user to know how to protect themselves online and what to lookout for to ensure his or her interactions online, remain private and is protected from malicious access.

With this given trend in adoption we are likely to see more home users infected with malware, more users having theirPCs compromised, more legitimate PCs and host used to relay attacks and lastly an increase of attacks emanating from local households.

3.1 Internet Connectivity and Data Subscriptions

According to the Communications Commission of Kenya (CCK) ICT Sector Quarterly Statistical Report for the second quarter (OCT-DEC 2013) of the financial year 2013/2014, the quarter under review witnessed growth in internet/ data subscriptions of 13.0 per cent to post 13.1 million subscriptions up from 11.6 million subscriptions registered during the previous quarter.

Internet/Data Subscriptions	13-Dec	13-Sep	Quarterly Variation (%)	12-Dec	12-Sep	Quarterly Variation (%)
Total Internet Subscriptions	13,186,968	11,671,337	13	9,496,573	8,519,148	11.5
Mobile Data/Internet	13,090,348	11,580,065	13	9,406,843	8,436,578	11.5
Terrestrial Wireless Data/Internet	16,429	17,169	-4.3	23,814	23,780	0.1
Satellite Data/Internet	682	749	-8.9	684	531	28.8
Fixed DSL Data/Internet	12,014	11,537	4.1	10,807	10,842	-0.3
Fixed Fibre Optic Data/Internet	67,470	61,739	9.3	54,400	47,392	14.8
Fixed Cable Modem	25	25	0	25	25	0
Total Internet Users	21,273,738	19,162,055	11	16,236,583	14,553,378	11.6

Table 15: Internet Subscriptions and Internet Users

According to the report, mobile data/internet sector has maintained its largest share of 99 percent of total internet subscriptions which could be as a result of factors such as the development of 3G network, social networking among others.

Internet users

Similar to the growth trend observed in data/internet subscriptions, the number of estimated internet users increased by 11.0 per cent during the quarter under review to record 21.2 million users up from 19.1 million users estimated in the previous quarter. A similar proportion of growth of 11.6 per cent was registered during the same period of the previous year.

Likewise, by the end of the quarter, the population that had access to internet stood at 52.3 per cent up from 47.1 per cent recorded in the preceding quarter representing growth of 5.2 per cent. This growth could have been as a result of increased uptake of ICTs that have catered to both social and economic needs and activities of the users.

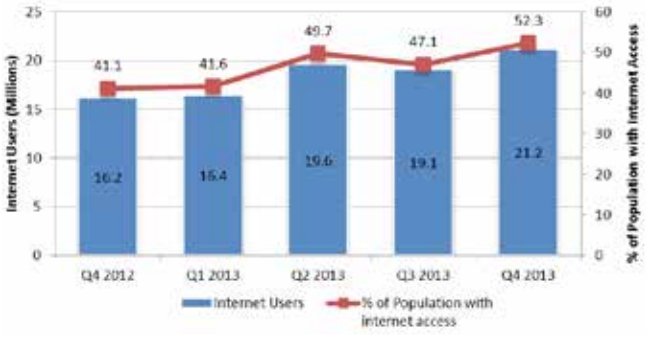


Chart 21: Estimated Number of Internet Users and Internet Penetration

3.2 Government targeted Cyber attacks

The Kenyan government has not yet defined a clear strategy on the protection of critical infrastructure including telecoms, transport, energy and financial services. This is a clear indication of the vulnerability of the country to cyber terrorism.

3.2.1 The banking regulators website hacked in July 2013

In July 2013, The Banking regulators website was attacked by hackers claiming to be from Gaza.The hackers seemed to have targeted the exchange rates section of the site which was flooded with messages in both English and French in a marquee that scrolled through the site. The hacking blocked many visitors from around the world who use the site to access exchange rates information for business or travel purposes. The site was however restored hours after the attack.

3.2.2 Transport Ministry website hacked

In March 2014, The Ministry of Transport website was hacked on raising concerns over the security of government websites. Visitors to the site were welcomed by an image that read "All Muslims are together, the CYBER WAR will be appeared in all countries which are not respecting Islam".

3.3 Hate Speech and Tribal Messages

In 2013, immediately after the elections, The National Cohesion and Integration Commission (NCIC) noted that the discussions in the social media had intensified along ethnic dimensions. At that time they increased their engagement in social media and tracked persons who perpetrated ethnic hatred with a view to recommending them for prosecution. According to the National Integration Cohesion Commission Act of 2008 hate speech includes using threatening, abusive and insulting words, behavior, displays or written material, publishing or distributing such written material, distributing, showing a play or recording of visual images or producing or directing a programme

which is threatening abusive or insulting that intended to stir up ethnic hatred. The Act makes hate speech a criminal offense for which offenders can receive up to 3 years in prison, a fine of not exceeding 1 million shillings or both. The continued use of social media by criminals is a worrying trend that must be addressed beyond NCIC. In 2012/2013 - a leading blogger was investigated by the law enforcement agencies for publishing defamatory posts on social media.Currently, Kenya does not have a dedicated social media law.

3.4 Cyber Bullying

Cyber-bullying refers to bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites.

Cyber bullying has become a major problem for Kenyans online. Everyday there are new cases reported of individuals who are cyber bullied. As more people embrace the use of social media, a minority are turning this into a bullying platform. In 2013, we noted an increase in cyber-bullying including use text messages or emails, rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles. Some of the victims of cyber bullying in 2013 included high profile individuals including a popular presenter with KISS 100 FM, Beauty Pageant contestant, a number of politicians and many other individuals.

3.5 Use of Social Media by Terrorists

On December 7, 2011, Al-Shabaab reportedly began using the Twitter social media network. Al-Shabaab joined twitter to counter Kenya's military spokesman Major Emmanuel Chirchir, who was updating journalists and the public through Twitter after his forces invaded Somalia. The account, HSMPress, has attracted over eight thousand followers for its witty taunts of the Kenya Defence Forces in general and its official spokesman, Maj. Emmanuel Chirchir, with whom it has frequent exchanges, in particular.

Twitter has given al-Shabaab an effective tool to spread its propaganda and empowered internal factions, giving them a potent voice of dissension that Somali citizens, group members and the world at large could easily reach and hear. During the deadly attack on the Westgate Mall al-shabaab live-tweeted the assault, a move that revealed how social media can be used by criminals to spread propaganda.

SERIANU

INFORMATION SECURITY AWARENESS AND TRAINING

Raising Awareness to Change Behaviour and Protect the Business

Our service will enable you to:

- Reinforce good security practices.
- Reduce the number and extent of information security breaches.
- Build a culture of information risk and security competence.
- Improve overall compliance with policies and procedures.
- Demonstrate management's commitment to secure information resources.
- Providing current staff with updated information on emerging risks.
- Facilitate internal discussion on information risk and security.

Background

One of the greatest threats to information security is inadvertent violation of basic information security precautions by well-meaning, non-malicious, uninformed employees. Whether it is storing confidential data unencrypted on a removable device that may be lost or stolen—or simply sharing proprietary information in a crowded elevator—inappropriate employee behavior is most often at the root of security breakdowns. These uninformed users can do harm to your network by visiting websites infected with malware, responding to phishing e-mails, storing their login information in an unsecured location, or even giving out sensitive information over the phone when exposed to social engineering.

The Serianu Information Security Awareness and Training Service

The Serianu Information Security Awareness and Training approach provides security training to the key stakeholders, administrators, and users who use/maintain or have access to company information. The training helps users and stakeholders to use, administer and maintain the technology solution on an on-going basis. It also provides the selected core technical staff with sufficient skills and competencies necessary to enable them anticipate, detect, respond and contain security threats after the training exercise.

Our Approach

The security awareness and training service is broken into a four-step process.

1. **Security training and needs assessment**
   This phase enables Serianu to properly align the requirements and supporting information with an approach that builds a defendable and measurable business case for the information security awareness program. In this phase we will identify:
   - Organisational training requirements
   - Management and staff needs analysis
   - Current Training inventory
2. **Design Security Training and Awareness Program**
   Using the information

collected and defined from the needs assessment, we will define the scope, objectives, participants, and responsibilities of the awareness program and creating an identity for the program. A well-constructed charter will provide the foundation for the program by factoring in all organizational requirements and considerations needed to meet its objectives.

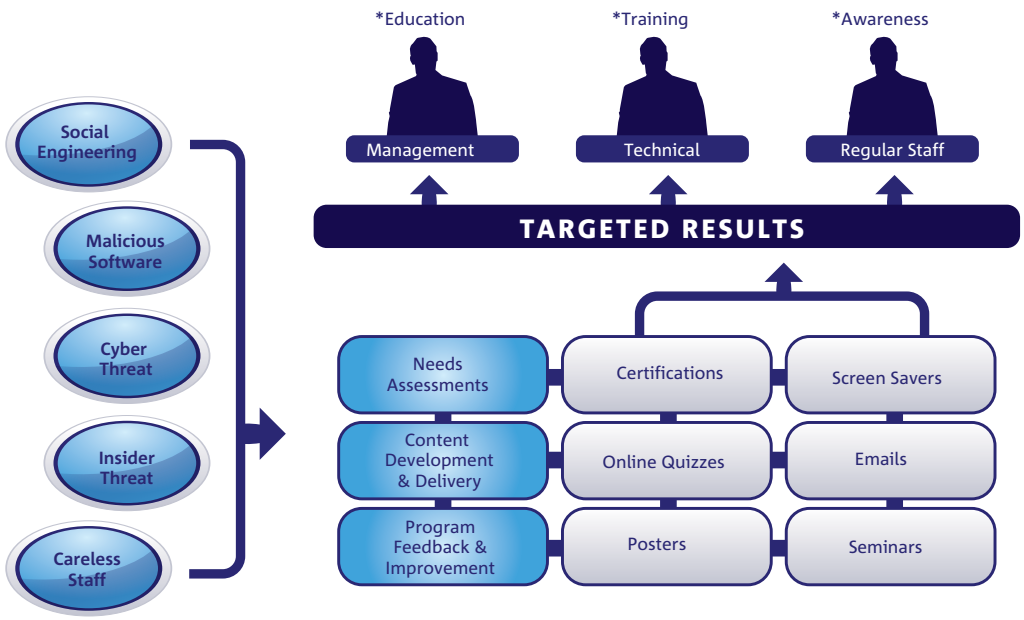
3. **Develop security training and awareness material**
   We will then develop a high-level design that captures the objectives for the course, lists the resources and subject matter expertise requirements, and begins to outline the instructional treatment best suited to meet the stated goals. The curriculum will be important in determining sources of training material to build.

4. **Implementation support**
   The implementation support provided will vary based on the type of training developed. Instructor-led training will have a different delivery and evaluation mechanism compared to web-based training. Nonetheless, all delivery mechanisms will follow the same fundamental steps which include a preliminary run with your company's stakeholders, a release to learners, and an evaluation or assessment mechanism. This evaluation step is important and will vary based on the intended awareness/training level. The information collected will be used to help assess and refine the curriculum.

Through these four steps, Serianu's best practice-based approach ensures the company is able to provide employees and general company staff with a thorough and operational knowledge of information security. Some of the topics covered during the session include; Information Security and Risk Management; Company Information Security Guidelines and Policies; Identity Theft and Social Engineering; Email and Internet Safety; Password Management & Access Control; and, Physical Security and Other Considerations

Conclusion

Security awareness training, when implemented correctly, is an important necessity for any organization. If the user base is properly informed as to what to watch out for, prevention and remediation procedures, will prevent a lot of potential problems that could affect the infrastructure and the company as a whole. The Serianu information security awareness and training offering ensures that your organisation is protected from accidental violations.



The Serianu Information Security Awareness and Training Service Diagram.

Section 4: Regulation and Policy

Cyber security efforts in themselves without clearly defined national frameworks, strategies and enforcement will not succeed. From the Kenyan government we have seen the introduction of cyber security plans and strategies that will provide a backbone for cyber security efforts and initiatives in Kenya. The mentioned frameworks play a critical role in shaping cyber security in the country. It is such frameworks that will guide in developing legislation that will assist in providing guidelines on ones conduct and expectations while online. It would be interesting to see how the strategies will assist in developing legislation tailored exclusively for cyber – crime mitigation in Kenya taking into consideration the challenges we are currently facing in managing cyber fraud.

4.1 COMESA - Cyber Security Strategy

Over the past years, the total amount of revenue lost through cybercrime activities such as credit card fraud globally and within the region is estimated to be close to $1 trillion. With increase in use of technology and new forms of organized cybercrime, the rise is inevitable.

As such, the Common Market for Eastern and Southern Africa (COMESA) developed the COMESA Cyber Security Program whose main objective is to provide effective public-private partnership for cyber security to create more secure network environments through better, standardized security programs.

The Cyber Security and Public Infrastructure Summit that was held in Kenya late last year (2013) brought together regional leaders to discuss harmonization of Cyber Security policies. It aimed at facilitating creation of holistic controls to detect and contain malicious activity within the region's critical information and infrastructure in a timely manner. The involvement of the judiciary will ensure that legislation and regulations for cybercrime are enforced.

4.2 Kenya Cyber Security Master Plan (CSMP)

In Kenya, the Cyber Security Policy is currently steered by the ICT Authority (Formerly the ICT Board) through the National Cyber Security Master Plan (NCSMP).

Kenya has taken the first step towards building a cyber security framework to suit Kenya's unique cyber threats. The key elements of the policy address are Training & Awareness, Economic Impact, Governance, Policy and Legal framework. The Kenyan government has sought help from the U.S, South Korea, Israel on various areas regarding cyber policy. The US provided guidance in building the NCSMP through Booz Allen & Hamilton, South Korea through Samsung provided the PKI infrastructure which was founded on the PKI policy. Israel provided technical training on various aspects of cyber security to a token government officials. The problem with such trainings is that the knowledge remains with individuals who aren't directly concerned in either implementing or executing the function.

Currently the government is not explicitly working with academic entities. Parterships into cyber security are mostly being undertaken by the private sector where partnerships are being forged to either increase the depth of research in cyber security or develop training and awareness curricula. The cyber security operations are at the moment handled by the government through the CCK which is fed by sector-CIRTs.

Kenya's biggest cyber crime is financial fraud which is at the top of the government's list of threats. Cyber Security is a serious problem for Kenya for various reasons. Firstly, we have great proliferation of bandwidth down to the grassrootsand this in turn opens up the country to the world. It does come with it's share of vices since there's little or no cyber security training/awareness among the general public. Secondly, organizations are facing serious internal threats in propergating cyber crime which directly affects the economy in terms of financial losses.

There are a large number of foreign attacks where foreigners are breaking into government and corporate websites unabated. Domestic threats are also on the rise since people living in Kenya are becoming more aware of how to carry out various cyber attacks. Most of the foreign attacks are merely done by script kiddies, people with

minimum knowledge on running tools to perform exploits. The goal isn't defined and it's purely for bragging rights. It can be argued that a lot of the targetted systems don't hold much valuable information so they have not become a target for determined hackers.

The government plays a key role in responding to these cyber threats and this can be done in the following ways:

First of all there needs to be a framework of reference to matters regarding cyber security. The National Cyber Security Master plan has been drafted awaiting implementation. The draft addresses how the government should respond to the threats, address training and awareness and also continously monitor its effectiveness.

The setting up a Cyber Security Command Centre in Kenya is inevitable for a growing economy such as ours. The threats faced by the U.S and Kenya are definitely diverse in both nature and magnitude. While we may not have superior threats, the Cyber Security Command center will be undeniably a focal point in defending the country against cyber crime. It would be able to address avert types of terrorist activity through monitoring and information intelligence. The government cannot achieve this by it's own. It needs to partner up with private entities and academia mostly because of innovative Research and Development and also knowledge management.

The Kenya Computer Security and Incident Response Team (KE-CSIRT) is currently partially operational and there's quite a lot that needs to go into getting it fully running. However the Kenya ICSIRT is doing commendable work with respect to creating a safe cyber environment in Kenya. The effects of the KE-ICSIRT are still yet to be fully felt due to various constraints such as capacity and requisite skills. Engagements with other relevant parties is also one challenge being faced by the organization. The KE-CIRT needs to buildsolid relationships with corporates, consultants and academic bodies in order to make a substancial impact, otherwise it will lose it's relevance.

As far as the availablity of Cyber Security Experts is concerned, there are few in the country. However as few as they may be, there is room to build capacity within our borders and only reach out for foreign help if it is really necessary. The first step is for the government to acknowledge the fact that they need assistance. The next step would then be to identify the local experts in the various areas and formally engage them and of course renumerate accordingly. We have private consultants ready to steer the country in the right direction regarding matters of cyber security. However the government's cavalier approach towards this subject may make it discouraging and disheartening if a proper methodology is not set in place to facilitate this effort.

There is a forensics lab under the CID which looks into forensic investigations for computer systems and mobile devices. However, from a reliable source, the knowledge and capacity to extract data from seized media is wanting and hardly reliable. There are personel trained in the CID who perform this exercise with some forensic tools that are not as bleeding edge as they should be. The challenge has been employing people whose passions are not grounded in the job they get. Meaning that to them its just another day job. Cyber crime experts are people who live and breath the very passion they are pursuing. Someone who will go beyond the normal call of duty. These are the individuals who will drive Cyber Security in Kenya.

4.3 Cyber-crime bill

In recent years Kenya has seen a marked increase in the number of cybercrime incidents. These crimes threaten national security and information, communication and technology infrastructure as well as Kenyan citizens' privacy and safety while accessing online resources.

The ministry of Information estimates that close to 2Billion Kenya shillings are lost annually due to cybercrime. Cybercrime comes in many forms but can be defined as any crime dealing with computers and networks whereby the computer is the subject of the crime.

In June 2013, a committee was formed to spearhead efforts against cybercrime under the Communications Act of Kenya. The Kenya Information and Communications bill 2013 incorporated and defined the term cyber security in the amendments further stipulating the penalties of the crimes for both individuals as well as organisations found committing them.

Following this, the office of the Director of Public Prosecution (ODPP) established a dedicated unit to tackle the prosecution of cyber criminals. The ODPP is also organizing a workshop to review existing laws and develop a complete draft bill on cybercrime based on international best practices.

This is a good indicator that the Kenyan government has taken the necessary preliminary steps towards securing our information, communication and technology infrastructure.

Conclusion

Kenya's cyber security challenges have been building for many years and they derive from the failure of organizations to recognize the severity of cyber security threats or to develop security programs to mitigate those resulting risks. They are also a result of product vendors failing to integrate security into their solutions. Short-term patches and fixes can be useful in response to isolated vulnerabilities, but they do not adequately protect critical infrastructure or data.

As the country moves forward, an understanding of the increasing security risks and how to manage and mitigate them must be emphasized and accelerated at all levels, from government, internet service providers, public and private organizations, citizens to students. Organizations must also establish and maintain adaptable security policies, processes, and infrastructure that can be used to coordinate response to ICT security threats. There is a strong need for defined security processes, better intelligence and continuous monitoring. There is also a need for continuous training to ensure current technology and security practitioners receive more in-depth training needed to secure critical ICT infrastructure. As a country we need to retain information security experts to guard our technology infrastructure. Businesses also need to retain security experts in the same way they outsource perimeter security to traditional security company. This would be the best way to ensure continued internet security in an ever changing world. It is imperative to take action before the situation worsens and the cost of inaction becomes even greater.

References

http://securityaffairs.co/wordpress/19368/cyber-crime/cyberbulling-infograph.html

http://www.cio.co.ke/news/main-stories/103-Government-of-Kenya-websites-hacked-overnight

http://www.actionfraud.police.uk/fraud_protection/identity_fraud

http://iwpr.net/report-news/kenya-social-media-no-forum-hate-speech

http://www.reuters.com/article/2013/02/05/kenya-elections-socialmedia-idUSL5N0B4C4120130205

http://www.theeastafrican.co.ke/news/Kenyan-banks-lose--18-8m-to-savvy-fraudsters/-/2558/2057524/-/gfy7g3z/-/index.html

http://www.africareview.com/News/Kenya-agency-alarmed-by-social-media-hate-speech/-/979180/2281992/-/format/xhtml/-/17v7ao/-/index.html

http://www.standardmedia.co.ke/?articleID=2000102398&story_title=dpp-declares-war-on-cyber-crooks

http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1539

http://www.itnewsafrica.com/2014/01/kenya-creates-special-cyber-crime-unit/

http://cio.co.ke/news/main-stories/what-does-kenyan-law-say-about-cyber-bullying

SERIANU

SERIANU CYBERTHREAT COMMAND CENTRE (SC³)

The Serianu CyberThreat Command Centre (SC³) monitors activities and events in client environments to ensure that anomalous behaviour is detected, identified, classified and acted upon where appropriate. Security engagements are co-managed where actionable behaviour is recommended in the event of malicious activity. Ongoing reviews of all activity and reports provide technical security oversight to detect meaningful data versus non-threatening anomalies. Client control environment procedures are also monitored to ensure that breaches of these procedures and the possible precursors of malicious activity are identified and reported.

PROTECT AGAINST MALICIOUS THREATS

The Serianu CyberThreat Command Centre (SC³) focuses on security and compliance. Security monitoring at Serianu guards your critical systems, seeking out any indicator of malicious activity from intruders that can threaten or even paralyze the very core of your business. Serianu will alert you immediately should a potential security breach be detected that could compromise the integrity of your network and can assist with remediation. It's a cost-effective, peace-of-mind solution to safeguard your network and your business' essential data.

Daily and monthly reporting provides the documentation required to demonstrate that threatening anomalies are detected and acted upon, while compliance also demands that all events have also been recorded and identified accordingly.

In the event of threats, Serianu provides actionable behaviour to counteract the event. Serianu will also provide forensics where appropriate, and maintain the proper evidence for legal action.

In order to successfully co-manage our clients' security, Serianu offers to assess our clients' environment to assist with defining the balance between security, compliance, best practices and budgetary constraints. Our Enterprise Security Services perform comprehensive testing and audits and provide the security solutions to protect your business-critical systems including:

The services offered by the SC³ allow us to identify, plan appropriate answers and react to cyber threats, often already installed within organisations' information systems:

- Event security monitoring
- Incidents detection and management
- Maintenance of systems in secure conditions
- Cyber Intelligence, threat and vulnerability monitoring
- A priori analyses of the compromised network and a posterior analyses of the extent of attacks
- Audits and tests (technical infrastructure)
- Crisis management assistance
- Security and footprints indicators provisioning

www.serianu.com