AN INTRODUCTION TO CYBER-SECURITY
THE LEGAL PERSPECTIVE

CPD: TRANSPORT, ICT AND COMMUNICATIONS

PRESENTED BY: JULIET WANGUI MAINA

FRIDAY 9th SEPTEMBER 2016
AREAS FOR DISCUSSION

- What is Cybercrime?
- Cost of Cybercrime
- Cybersecurity
- Current Legal and Regulatory Framework
- Proposed Computer and Cybercrime Bill 2016
- Cybersecurity in an organization
- Future Promising Practices
- Emerging Vulnerabilities
INTRODUCTION

Cyber-crime - criminal activity in which computers or computer networks are a tool, a target or place of criminal activity and include everything from electronic cracking to denial of service attacks.

Cybercrime also includes traditional crimes in which computers or networks are used to enable illicit activity.

Cybersecurity is defined in the Kenya Information and Communications Act (2013) as "the collection of tools, policies, security concepts, security safeguards, guidelines, actions, training, best practices that can be used to protect the cyber environment"
1. Government
2. Banks
3. Financial services and mobile money
4. Manufacturing
5. SACCOs
6. Telecommunications sector

Source: Kenya Cybersecurity Report 2015 (Serianu)
EVOLUTION OF CYBERCRIMES

- Traditional approaches to cybercrime
- Everyday there are new emerging channels for criminals

95%

“95% of all attacks on enterprise networks are the result of successful spear phishing”
Source: Allan Paller, Director of Research - SANS Institute

90%
COST OF CYBERCRIME

The cost of cybercrime can be assessed directly and indirectly taking into account various issues such as:

- Loss of financial assets and sensitive business information
- Loss of personal identity information
- Reputational damage to the organization
- The loss of intellectual property
- Opportunity costs – Service disruption
- Additional costs for securing networks

Cybercrime extracts between 15 and 20% of value created by the internet – Microsoft (2016)

In 2015, Kenya lost KShs. 15billion to cybercrime, with 4billion of it taking place within the banking sector – Kenya Cybersecurity report 2015 (Serianu)

Cyber Crime Costs for Businesses Projected To Reach $2 Trillion by 2019 – Forbes (2016)
## LEGAL AND REGULATORY FRAMEWORK

### Current Legal Framework

<table>
<thead>
<tr>
<th>Law</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kenya Information and Communications (Amendment) Act (Cap 411)</td>
<td></td>
</tr>
<tr>
<td>Evidence Act (Cap 80)</td>
<td></td>
</tr>
<tr>
<td>The Penal Code (Cap 63)</td>
<td></td>
</tr>
<tr>
<td>The Proceeds of Crime and Anti Money Laundering Act, No. 9 of 2009</td>
<td></td>
</tr>
<tr>
<td>The Criminal Procedure Law (Cap 75)</td>
<td></td>
</tr>
<tr>
<td>Central Depositories Act (2013)</td>
<td></td>
</tr>
</tbody>
</table>

### Proposed Bills, Policies and Regulations

<table>
<thead>
<tr>
<th>Bill/Policy</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Infrastructure Protection Bill (2015)</td>
<td></td>
</tr>
<tr>
<td>Data Protection Bill (2013)</td>
<td></td>
</tr>
<tr>
<td>National ICT Policy (2016)</td>
<td></td>
</tr>
<tr>
<td>ICT Capacity Bill (2016)</td>
<td></td>
</tr>
<tr>
<td>Computer and Cybercrime Bill (2016)</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity Regulations (2016)</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity and Protection Bill (2016)</td>
<td></td>
</tr>
</tbody>
</table>
PROPOSED COMPUTER AND CYBERCRIMES BILL 2016

Offences and Liability

Jurisdiction

Yes, we have “general” jurisdiction.

Investigative and Handling procedures

International cooperation
The following existing laws stand to be affected by with the enactment of the new bills:

- KICA (Cap 411 A)
- Evidence Act (Cap 80)
- Mutual Legal Assistance Act, No. 36 of 2011
- The Penal Code (Cap 63)
- The Proceeds of Crime and Anti Money Laundering Act, No. 9 of 2009
- The Criminal Procedure Law (Cap 75)
- The National Payment Systems Act, 2011
- The Sexual Offences Act, 2006
CYBERSECURITY IN AN ORGANISATION

**Executive level:**
- Institute sound cybersecurity strategy
- Ensure quality information is received and assimilated
- Implement user security awareness programmes
- Support strategy-based spending on security

**IT:**
- Conduct forensic readiness assessments
- Be aware of the changing threat landscape and attack vectors
- Test incident response plans
- Implement effective monitoring processes
- Employ new strategies: cyber attack simulations, gamification of security training and awareness sessions and security data analytics

**Audit & Risk:**
- Ensure a thorough understanding and coverage of technology risks
- Conduct up-front due diligence to mitigate risks associated with third parties
- Address risks associated with operational (non-financial) systems
- Address basic IT audit issues
ROLE OF LEGAL

MITIGATING RISK:
- Contractual management
- Compliance with regulatory requirements
- Develop a culture of cybersecurity

HANDLING INCIDENTS
- Forensic procedures
- Dealing with breach of contracts
- Employment issues
- Dispute resolution
- Intellectual property matters

IMPACTING THE LEGAL LANDSCAPE
- Track evolving cyber-regulatory environment
- Contribute where possible through public participation
TO SUMMARISE...

Legal is responsible for:

- Developing cyber risk management frameworks, to enable clients to assess their compliance with laws, regulation and best practice relating to cyber risk
- Preparing for cyber breaches, including designing tailored cyber response plans
- Responding post breach, including advising the board on internal and external actions, coordinating investigation of the breach and liaising with regulators and third parties
- Advising on how to comply with national and international technology regulations
- Understand the meaning of contracts for technology, including services, software and outsourcing.
- Anticipating legal risks and approach them appropriately.
- Exercise critical thinking to understand the practical implications of industry standards
FUTURE PROMISING PRACTICES

- Intelligence sharing and gathering
- Development of necessary collaborations between agencies
- Personnel development – capacity building
- Building a culture of cybersecurity through awareness
- Encouraging institutions to invest in cybersecurity
- Cybercrime insurance
- Collaborative incident response teams
EMERGING VULNERABILITIES

Virtual currency - bitcoin

There are different types of wearables

Internet of things

Wearable technology

Cloud computing and big data
THANK YOU

www.tripleoklaw.com
jmaina@tripleoklaw.com