

# Effective Board Cyber Security Governance

Presentation by:

Nasumba Kwatukha

CPA,CIA, CISA,CFE,CRMA,CISSP,IIC

# Menu



- ☐ *Definition of Governance;*
- ☐ *Definition of Cyber Risk and Cyber Security*
- ☐ *Cyber Security Risks*
- ☐ *Role of Board in Cyber Security*
- ☐ *Link Cyber Security to Governance and Strategy*
- ☐ *Way forward*
- ☐ *Q &A*

# Governance



*“If you know your enemies and know yourself, you will not be imperiled in a hundred battles.”*

*Sun Tzu*

# Governance



*Governance is the Stewardship of an organization, establishment of Policies and ensuring that objectives are achieved through a controlled environment.*

- *Executive Leadership*
- *Board Accountability*
- *Incident Response Team*

# Cyber Crime



According to the International Organization of Securities Commissions (IOSCO),

*‘cyber-crime’ refers to a harmful activity, executed by one group or individual through computers, IT systems and/or the internet and targeting the computers, IT infrastructure and internet presence of another entity*

*Confidentiality, Integrity, and Availability.*

# Cyber Risk and Security



*Cyber risk is any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems*

*Cyber Security can be defined as an activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation*

# Emerging Risks



WikiLeaks

 **bitcoin**



# Emerging Risks

❑ KRA

❑ NSIS-I was in Nairobi and Working(Goose Chase)

❑ IEBC- Sleeping Servers and Canaan Journey

## *STATISTICS*

*18 Billion-Research by Serianu (Kenya Cyber Security Report)*

## Welcome to Internet Banking

User ID:

Password:

Select Language:

Login

[Forgot your security details?](#)  
[Log on Help?](#)

 (+254) 705 325 325 / 737 325 325

 [customerservice@familybank.co.ke](mailto:customerservice@familybank.co.ke)

[Privacy & Security](#) | [Terms & Conditions](#) | [Contact Details](#)



# Challenges with Cyber Crime



- ❑ *Geeks unlike the Street Robber*
- ❑ *Evidence gets lost Quickly- Time outs and Tempering*
- ❑ *Proliferation of Tools through Internet*
- ❑ *Evidence Act threshold*
- ❑ *Poor Guardian :Mulika Mwizi*

# Emerging Cyber risks



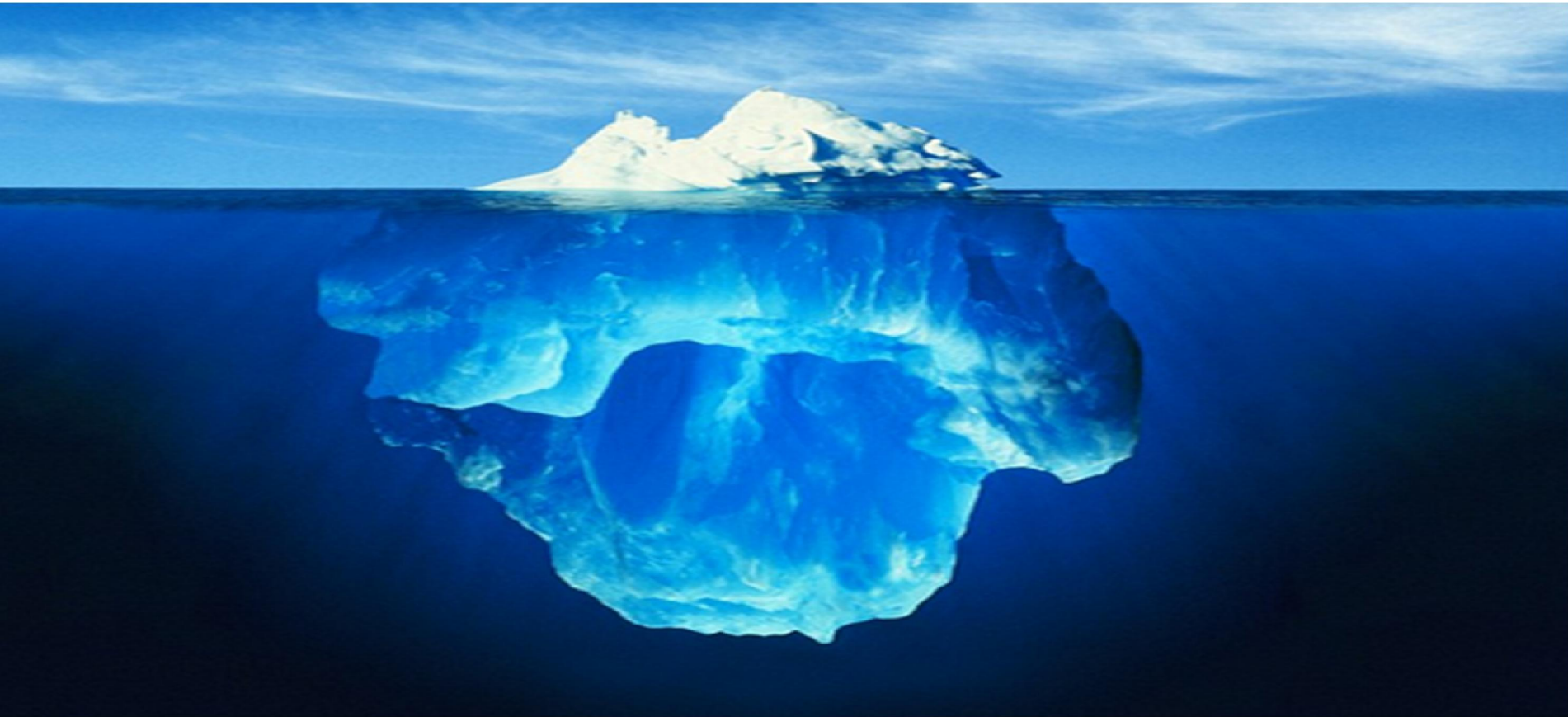
- ☐ *A breach in institutions' databases exposing data to cyber criminals*
- ☐ *Improper access to privileged accounts –Network Scanning tools-Active Directory; Terminated Passwords and emails*
- ☐ *Sharing IP addresses*
- ☐ *Deleting log files or disabling detection mechanisms.*
- ☐ *Interconnectedness of institutions could lead to compromise in the institutions entry- Bluetooth, Online signatures*
- ☐ *Segregation of duties and Roles*

# Emerging Cyber risks



- ☐ *Data replication arrangements that are meant to safeguard business continuity could transfer malware or corrupted data to the backup systems.*
- ☐ *Poor authentication controls and Access Logs: Identity Theft; Password Crackers*
- ☐ *Scripts and Back end Processes: Auto generate Invoices and Cheques*
- ☐ *Phishing and Whaling attacks*
- ☐ *Machine Learning enabled attacks*

What is visible vs what is hidden



# Role of the Board in Cyber Risk



*All board members should understand the nature of their institution business and the cyber threats involved. **‘tone from the top’***

*Robust oversight and engagement on cyber risk matters at the board level promotes security risk conscious culture within the institution.*

*Engage management in establishing the institution’s vision, risk appetite and overall strategic direction with regards to cybersecurity.*

*Allocation of an adequate cybersecurity budget based on the institution’s structure and size of its cyber risk function.*

# Board responsibility



*Review management's determination of whether the institution's cybersecurity preparedness is aligned with its cyber risks.*

*Adoption of an effective internal cybersecurity control framework with submission of periodic independent reports.*

*Establish or review cyber security risk ownership and management accountability and assign ownership and accountability to relevant stakeholders*

*Approve and continuously review the cybersecurity strategy, governance charter, policy and framework.*

# Governance Frameworks



## *Frameworks*

- ✓ *NIST Cybersecurity Framework*
- ✓ *NIST 800-Series Guidance*
- ✓ *SANS 20 Critical Security Controls*
- ✓ *ISO 27001*



# Link cyber security and business performance



- *Identify the actual risks*
- *Prioritize and protect*
- *Develop and sustain a cyber security program*
- *Enable business performance*
- *Optimize for business performance*

# Way Forward



- ☐ *Training*
- ☐ *Plan in the Risk Program*
- ☐ *Capable Guardian*
- ☐ *Regular Tests-Pen test, Vulnerability Assessments*

# ICPAK



## Q & A

SESSION 1

Nasumba Kwatukha

CPA,CIA,CISA,CFE,CRMA,CISSP,IHK

0728-771-497