Information Security Specialisation

Public Sector Attachment

Outline

1 Objectives

2 Ministry/State Corporation Structures & visions

3 Projects in the Ministries

4 Opportunities

5 Skills acquired in the Public Sector

6 Supervisors and Mentors

7 Challenges/Observations

8 Recommendations

9 Appendices

Objectives

- Identifying system vulnerabilities and reporting on security measures to be taken to address the threats.
- Analyzing security risks and developing response procedures as well as developing and testing software deployment tools, firewalls and intrusion detection systems.
- Developing security policies to address Information and Systems security covering BYOD.
- Resolving any security issues that occur in case of an incident
- Collaborating with the appropriate people for the purpose of recovery, risk mitigation or providing the needed information.

Visions

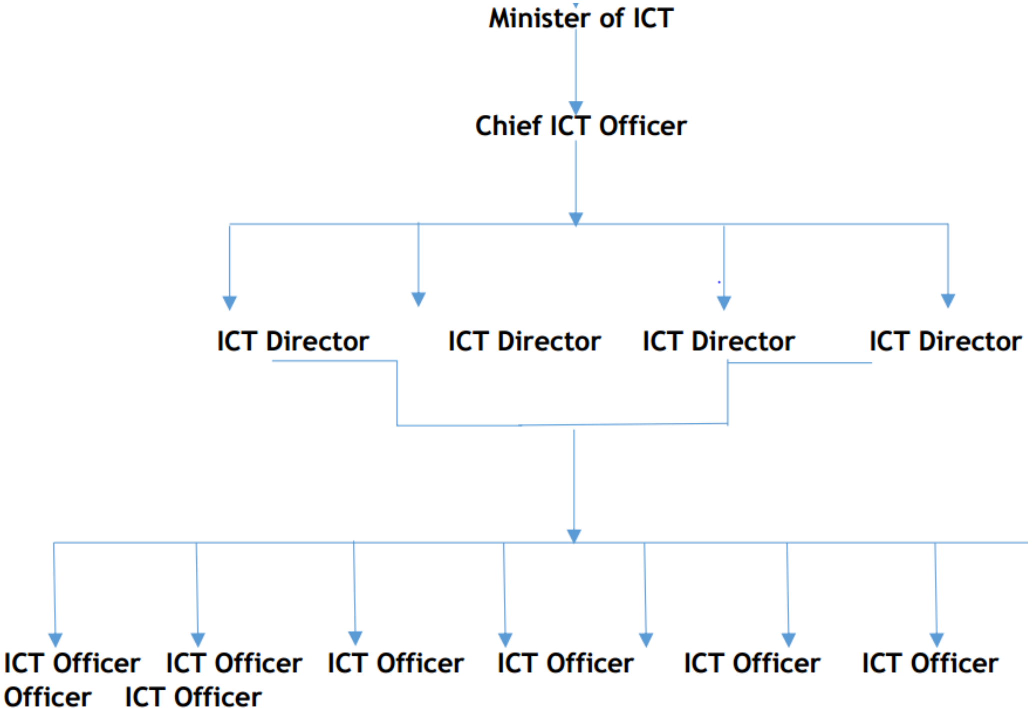
Government's Cybersecurity Mandate

- **To enhance the nation's cybersecurity posture** in a manner that facilitates the country's growth, safety, and prosperity.
- **To build national capability** by raising cybersecurity awareness and developing Kenya's workforce to address cybersecurity needs.
- **To foster information sharing and collaboration** among relevant stakeholders to facilitate an information sharing environment focused on achieving the Strategy's goals and objectives.
- **To provide national leadership** by defining the national cybersecurity vision, goals, and objectives and coordinating cybersecurity initiatives at the national level.

Alignment to the mandate

- National capacity building by training PDTP trainees in identifying system vulnerabilities and learning to identify breaches
- Fostering information sharing and collaboration by collaboration between ministries and various security teams during incidence response and information awareness
- Enhancing of the nation's cybersecurity posture with local capacity building and better collaboration amongst ministries for better effectiveness
- National leadership provided with the proposal of a Cyber crimes bill along with collaboration during incidences

Organisational Structure



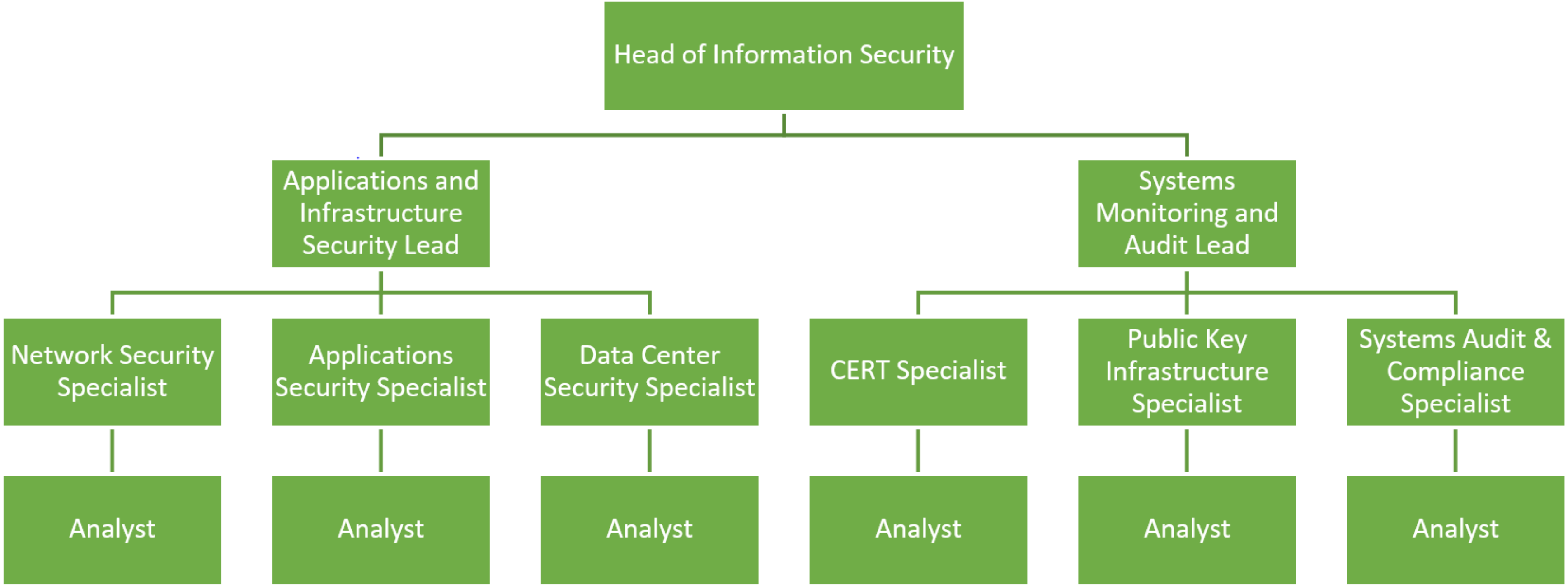
Minister of ICT

Chief ICT Officer

ICT Director ICT Director ICT Director ICT Director

ICT Officer ICT Officer ICT Officer ICT Officer ICT Officer ICT Officer
Officer ICT Officer

Information Security Division



Head of Information Security

Applications and Infrastructure Security Lead

Systems Monitoring and Audit Lead

Network Security Specialist

Applications Security Specialist

Data Center Security Specialist

CERT Specialist

Public Key Infrastructure Specialist

Systems Audit & Compliance Specialist

Analyst

Analyst

Analyst

Analyst

Analyst

Analyst

Projects in Ministries

- **Shirikiana shared services**
  - Cloud Infrastructure (Hybrid Environment)
    - Public cloud
    - Private cloud
  - Mail Services (Exchange/365)
  - Office365 Application suite
  - Windows Imaging (Customised OS package for specific ministries,depts,parastatals & Agencies)

- **Managed web hosting**
  - Providing hosting of government websites
  - Management of Government Domains
- **Incidence Response Team**
- **Network Monitoring**
- **GOK Cyber defence discovery**

Existing Systems

ORGANIZATION	SYSTEMS AVAILABLE
MINISTRY OF AGRICULTURE, LIVESTOCK & FISHERIES	-Live website -Company Intranet -Old e-subsidy system
NATIONAL CEREALS AND PRODUCE BOARD (NCPB)	-Navision (ERP) System -Cyberoam
NAIROBI CITY COUNCIL	-ElectronicDevelopment Management System (e-DPMS) -Traffic Surveillance -E-Payments
MINISTRY OF EDUCATION	-EMIS-Education Management Information System
ICTA	- Azure Shared Services - Web Server hosting

Opportunities

- Establishment of information security divisions ministry-wide
- Improved awareness on attack vectors through training across all ministries
- Improved collaboration with market sectors to improve the nation’s cybersecurity posture
- Improve information sharing and collaboration

Skills acquired

Technical skills	Organization Skills
Configuration of BYOD policy using MDM (Mobility Device Management) with Office365 and Microsoft Intunes	Understanding organizational structure and the roles of each position in the organization.
Cloud security - Working with Azure security centre. Monitoring logs and workloads on the virtual environment **Incidence response** - Identifying, analysing and responding to alerts	Soft skills – The soft skills include Teamwork, communication, Time management, leadership, planning etc.
Intrusion detection and prevention	Workplace ethics & collaboration skills
Security hardening of application, networks and endpoints	Employees welfare
Malware scanning and reverse engineering	Information Security Management. Risk-based approach to organisational security.

Challenges/Observation

Technology Issues/Observations	People issues/Observations
Outdated licenses and end-user systems- Employees should have latest updates on current OS, antiviruses, firewalls.	People still use their personal emails for official business communication which compromises or acts as a threat to sensitive data security
Unstable internet with several down times	Few professionals within IT office to manage a whole ministry.
Outdated server infrastructure & used of commercially licensed products	Intern recognition issues with other departments apart from the team

Challenges/Observation cont.

Technology Issues/Observations	People issues/Observations	Process Issues/Observations
Users do not always log off machines when they are not within the vicinity which can lead to unauthorized access.	Total lack of computer skills for some government employees.	Issue escalation is 1-way
	Resistance to Change from existing civil servants	Financial facilitation

Supervisors and mentors

- The supervisor makes sure we constantly have assignments allocated to us that are required to be accomplished, tested and used within the company
- We have learnt managerial and organizational skills e.g. delegating, planning, scheduling, follow-up
- Teamwork e.g. during repair and replacement of hard disks. The supervisor was there and we did it together.
- Technical skills e.g. upgrading the network systems from 2G to 3G
- Project management and reporting according to government protocols
- Being detail oriented and presenting facts in a logical manner

Recommendation

Technology	People	Process
Use of systems to manage processes instead of many manual systems.	Training and sensitization on the need for information security and how to manage ICT assets to minimize unauthorized access	Digitization of the manual processes
Regular updating of databases, system maintenance and patching	Create awareness on importance of securing information and devices.	
Adoption of new technologies	Employment of more ICT Skilled Professionals.	
Update firewall licenses, antivirus licenses		

Appendix 1: List of Team Members

Name of PDTP	Role in the team
Michael Muita Mugo	Writing the content and presentation
Mercy Gikonyo	Writing the content
Trevor Kaon	Content

Appendix 2: List of Security PDTPs and Organisations

Excel Sheet

Appendix 3: List of Site visits & Workshops attended

Visits/Workshops	Facilitating Organisation
IBM Security Intelligence	IBM
IBM Application Security	IBM
Sensitization to email phishing and attack vectors	NCC County
Azure Infrastructure as a Service	Microsoft (Technobrain)

INFORMATION SECURITY.

Private Sector Attachment

BY: ***ELIZABETH GETANGE.***

WYCLIFFE WANYANGU.

Outline

1 Objectives

2 Organization’s ICT Structure

3 Skills learnt in the Private Sector

4 Skills that can be applied in government

5 Supervisors and Mentors

6 Challenges/Observations

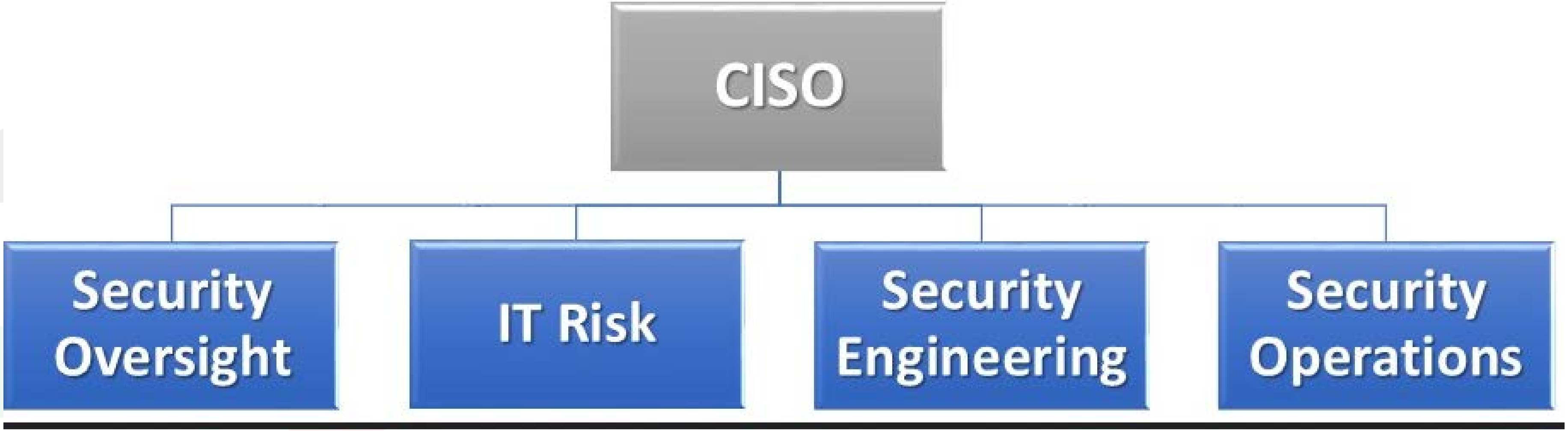
7 Recommendations

8 Appendices

Objectives

- Gain skills and experience from the company and identify new ways or systems that can be applied in public sector to improve service delivery.
- Understand the private sector setup and operation.
- Understand office organization and practices in private sector environment.
- Acquire skills for implementing ICT projects
- Understand the issues surrounding ICT service delivery.
- ICT department’s roles and their operation.
- Understand different roles and responsibilities of ICT staff in service delivery.

Organisational Structure



CISO

Security Oversight

IT Risk

Security Engineering

Security Operations

Skills learnt in the Private Sector

Technical skills	Organization Skills	Trainings attended
Information gathering	Understanding organizational structure and the roles of each position in the organization.	FireJumper for Cisco (Next Generation Firewalls and Next Generation Intrusion Prevention, Web and Email Security.
Malware scanning and reverse engineering	Soft skills – The soft skills include Teamwork, communication, Time management, leadership, planning, self-awareness, branding etc.	IBM Application Security
Intrusion detection and prevention	Workplace ethics	IBM Security Intelligence Analyst
Security hardening of application, networks and endpoints		

Skills that can be applied in government

Technology	People	Process
Web and email security	More Awareness of the possible attack – Attack vectors include social engineering, phishing, shoulder surfing, information leakage and malware attacks.	Clear operating procedures.
Policy and access	Governance and regulation	Defined security roles for easier issue escalation
Next Generation Firewalls and Next Generation Intrusion Prevention Security (NGFW & NGIPS)	Skilled personnel	Audit and compliance
Advanced Threat (DDoS, AMP, BYOD Security)		Access control

Supervisors and Mentors

Observations	Recommendations
➢ Resourceful. ➢ Proper guidance. ➢ Friendly ➢ Motivating	➢ Be enlightened on the PDTP objectives. ➢ Communication. ➢ Be prepared to onboarding PDTPs.

Challenges/Observations

Technology	People	Process
Unfulfilled expectations:- most of the expectations by trainees were unfulfilled since some private companies were more of business oriented rather than tech.	**Poor communication**: This applies to communication between ICT Authority and supervisors and between Management Interns and their mentors	**Proper planning-** lack of proper planning for the PDTPs for them to gain the most from the attachment.
Trust issues-Lack of exposure of trainees on security mechanism and technology in some private companies due to	The need to interact with the employees in various department not only that of IT so as to gain a variety of skills.	**Bureaucracy**
	Unwillingness of some employees to share their knowledge and skills concerning ICT security in some companies.	**Deployment process** to private sectors had a lot of challenges that need be addressed eg deployment letters to be issued on time.
	Poor cooperation from some mentors-: Some mentors don’t respond when contacting them.	**Time limit for private sector** internship was too short for one to gain more skills and experience on ICT security.

Recommendations

Technology	People	Process
More hands-on experience should be facilitated in the private sector so that the trainees can gain more skills and experience.	Good relations between interns, their supervisors and mentors should be encouraged.	Minimize procedures to reduce time taken to have issues resolved
Use of new technologies.	More trainings on ICT security should be encouraged for all the employees in the companies.	Proper control measures.
Partner with more private companies.	Continues ICT staff empowerment.- Encourage and reward results and effort.	
Advance security measures	Discourage laxity and complacence in public sector.	

Appendix 1: List of Team Members

Name of PDTP	Role in the team
Elizabeth Getange	Writing the content and presentation
Wanyangu Wycliffe	Writing the content

Appendix 2: List of Private Sector PDTPs and Organisations

Name of PDTP	Organisation
Kennan Obura	Oracle Kenya
Metobo John	Seven Seas Technologies
Jackson Mbogo	Bamba Group
Byegon Gilbert	Micropoint Systems
Kipkorir Cheruiyot Josphat	Huawei
Leparteleg Janet Silantoi	Soulco Kenya

Name of PDTP	Organisation
Kilenge Shadrack Muteti	Liquid Telecom
Moindi Duke Martin	Maramoja Transport Ltd
Waheire Alex Njogu	Dell EMC
Evans Ombati	Skylink Networks
Anne Muthoni	Bamba Group

Appendix 3: List of Site visits & Workshops attended

Visits/Workshops	Facilitating Organisation
IBM Application Security	IBM
IBM Security Intelligence	IBM
FireJumper	CISCO

Appendix 4: Photo at the working organisation

Appendix 4: Photo during field work