Always Use Protection: Play Your Role!

Edward Kakooza, Makerere University, Kampala Uganda
Dickson Muyumba, Makerere University, Kampala, Uganda
The Flow

- Definitions: Data & Information, Data & Information Loss
- Why safeguard Data & Information
- Impact of Data & Information loss
- Protective Measures
- Case Study
- Laws, Policies and Regulations
Learning Objectives

• Analyse the impact of information loss on the research industry

• Discuss possible protective measures for data and information loss
Definitions

Knowledge
Know-how, understanding, experience, insight, intuition, and contextualized information

Information
Contextualized, categorized, calculated and condensed data

Data
Facts and figures which relay something specific, but which are not organized in any way

Source: Theirauf (1999)
Definitions Cont....

Data & Information Loss

Any process or event that results in data being corrupted, deleted or made unreadable to a user.

Forms of Data & Information Loss

• Softcopies
• Hardcopies
Importance of Data
CIA Triad
Data is considered to be the most valuable asset and losing that data can be harmful to the long life of the Researcher, Research Administrator, Project & Organisation.

Although there so many unforeseen consequences of data loss, most of these are not obvious until after a data loss event occurs.

As Joni Mitchell once sang; “You don’t know what you’ve got ‘till it’s gone. It is always important to ensure that you backup your critical business data regularly, safely & in a restorable form.
Data & Information Loss

- Unauthorized Access
- Hard Drive Formatting
- Software Corruption
- Disaster
- Liquid Damage
- Computer Theft
- Hard Drive Damage
- Power Outages
- Viruses & Malware
- Human Error

Data & Information Loss
Human Error – Filing systems

• We all make mistakes and sometimes they’re big ones.

• Mistakes can result in the unintentional deletion of data files, overwrite important files.

• Human error also play a role in many other main causes of data loss, including hard drive damage, liquid spills, software corruption and hard drive formatting.
Viruses & Malware

- Viruses & Malware are often thought about after the problem has occurred.
- Viruses steal or delete data and can bring operations to a standstill.
- Email-based attacks, Moving Flash disks
- Ransomware
Hard Drive Damage

- Hard drives are the most fragile parts of computer systems

- Majority of data losses occur due to hardware malfunctions
Power Outages

- Unstable power flow & Fluctuation especially in LMICs
- Interrupt operations substantially, shutting software systems down without warning.
- Result in the loss of unsaved data, but it can also cause existing files to be corrupted due to improper shutdown procedures.
- If a computer shuts down while it is writing to the hard drive system, it may never start up again.
Computer Theft

- Use of laptops or smartphones rather than desktop computers.

- Laptop theft is a serious risk and can happen anywhere if a laptop is left unattended.

- On top of losing data, laptop theft also poses the threat of a data breach.
Liquid Damage

• With the busy work schedules today, drinks and computers are inseparable.

• Spilling coffee or water on laptops or computers can cause a short circuit, making it difficult to recover your computer, let alone the data stored inside.
Disasters

• Like the word goes disasters can happen when you least except them.

• They can destroy your computer, your data and even your entire organisation.

• Natural disasters can cause irreparable damage to organisation if data is not backed up.
Software Corruption

- Unexpected or improper software shutdowns may seem innocent on the surface but can cause serious issues for your data.

- Improper shutdowns can corrupt your data or delete your progress, wasting time and losing valuable data.

- When software is corrupted it may not be able to run again, meaning you cannot access data stored in that software.
Hard Drive Formatting

- Accidental formatting of your hard drive can cause you to lose data instantly.

- Research Administrators can format a hard drive by accident if they misunderstand system prompts or error messages.

- Reformattting can also occur during system updates and result in data loss.
Unauthorized Access

• Hacking and data breaches have become a much more common problem today.

• Unauthorized guests in your network can cause serious damage to your data, deleting and stealing any data they wish.

• Sometimes data can be stolen or compromised by employees themselves or other insiders.
Why safeguard Data & Information
Why safeguard Data & Information

• Research data is very crucial!

• It can be used by a number of people including Policymakers.

• Safeguarding data and building trust in how it is used is an essential part of using data effectively to support Research Industry.
Why safeguard Data & Information

- A data breach at an organisation can result into loss of top secret information & tracking of organisation’s progress.
Impact of Data & Information loss
Consequences & effects of Data loss to Organisations

• If your data loss is due to malware or hackers, then you run the risk of identity theft.

• Loss of trust

• Affects research productivity.

• Breach of research participants’ confidentiality
Consequences & effects of Data loss to Organisations Cont …

• There is a famous saying, “There’s no such thing as bad publicity,” however, this doesn’t apply to a data loss scenario.

• Cost related to data recovery & repairs are huge.
Protective Measures for Data & Information loss
Protective Measures Cont..

Minimum benchmark standards for Computer & Information Security

User Sensitisation

Collaborative Data sharing Agreements
Protective Measures Cont..

Close working relationship with IT Personnel
Protective Measures Cont..

Use anti-virus software – This is essential to prevent viruses and malware from infecting your computer. Be sure to keep anti-virus software updated so it runs properly and effectively.

Keep your computer clean & dry - Dust or moisture collecting in a computer can cause the hard drive to crash or computer to overheat. Store all computers and laptops in dry, ventilated areas.
Partition your Hard Drive - Partitioning means creating separate program and data zones. This means that if the program portion of a hard drive crashes, you may be able to recover the data because it is stored in a separate location.
Physical Protective Measures Cont..

Control employee access - All employees working with organisation data should be properly trained about confidentiality or how data can be shared.

It is in the best interest of your Organisation to control who can access different levels of data to protect from accidental or intentional data loss.
Physical Protective Measures

For the most effective backup plan, store your backups in a physically separate location to prevent the risk of data loss from physical destruction or theft.

Backing up data means that you have at least one additional copy of all important data.
Good Clinical Practice

Data Quality & Integrity

Accurate reporting, interpretation, and verification

Encourages confidentiality of records
What has been Done.
Makerere University Legal Unit
Directorate of ICT

GET ANSWERS...

...and quickly fix all or most of your IT related issues. Check out Our IT Self Help Knowledge Base (answers.mak.ac.ug)
Trainings, Awareness Campaigns
RENU Data Center

Colocation

RENU member institutions can now host their servers in any of RENU’s secure data centers for off-site disaster recovery, or for any other desired solution, at very competitive rates. The high availability of both the data center power and the dense network of high-speed optical fiber links ensures that the institution is able to access their off-site services at all times.

Data transfer between a member institution connected to the RENU network and their off-site servers in the RENU data centers can reach rates (speeds) as high as 10 Gbps and is tariff-free. The latency between member institutions connected to the RENU network and the RENU data centers is as low as 1 ms (for campuses in Kampala) and as high as 25 ms (for the farthest upcountry campus in Uganda).

The data center security, high availability, very low latency, high data transfer rates and the tariff-free transfers set colocating in the RENU data center apart from the others.
The RENU cloud offers highly available server platforms supporting both Windows and Linux-based environments. These virtual servers are hosted locally in Uganda and on the RENU network making the RENU Cloud an institution's ideal hosting platform.

The resources provisioned include virtual CPUs, virtual RAM and virtual hard drives, and are billed according to the computing environment or package selected.

The RENU Cloud also serves as a good solution for member institutions that wish to have offsite disaster recovery solutions without incurring the heavy costs of building offsite data centers and buying server hardware.

Data transfer between the RENU Cloud and a member institution connected to the
A globally competitive Uganda enabled by Information Technology

Home » Laws & Regulations

Laws & Regulations

I.T Certification of Providers of I.T Products and Services (Amendment) Regulations, 2018

Computer Misuse Act 2011 (Act No. 2 of 2011)

Data Protection and Privacy Bill-published

Electronic Signatures Act 2011 (Act No. 7 of 2011)

Electronic Signatures Regulations 2013 - SI 43 of 2013

Electronic Transactions Act 2011 (Act No. 8 of 2011)

Electronic Transactions Regulations 2013 - SI 42 of 2013

NITA-U Act (Act No. 4 of 2009)

NITA-U (Authentication of IT Training) Regulations 2016 - SI No. 70 of 2016

NITA-U (Certification of IT Providers and Services) Regulations 2016 - SI No. 69 of 2016

Opportunities (Tenders & Jobs)

Thursday, September 26, 2019 - 12:37

BID NOTICE UNDER OPEN BIDDING: SUPPLY OF TABLETS & LAPTOPS FOR NITA-U Staff - NITA-U/SUPPLS/19-20/00649

Tuesday, September 17, 2019 - 13:63

ADDENDUM NUMBER 1 FOR THE SUPPLY, CONFIGURATION, CUSTOMIZATION, OPERATION AND MAINTENANCE OF DIGITAL AUTHENTICATION AND ELECTRONIC SIGNATURES SOLUTION FOR THE GOVERNMENT OF UGANDA
Guidelines & IT Standards

- The Cloud Computing Guidelines for GOU
- NITA-U Standards Catalogue 2017
- The Online E-Safety Educational Toolkit for Young People in Uganda
- Guidelines for Development and Management of Government Websites
- Guidelines for Operation, Usage and Management of IT Infrastructure in MDAs & Local Government
- Government of Uganda Social Media Guide
- Standards for Structured Cabling for Government MDAs
- Guidelines and Standards for Acquisition of IT Hardware & Software for MDAs

Opportunities (Tenders & Jobs)

- **BID NOTICE UNDER OPEN BIDDING: SUPPLY OF TABLETS & LAPTOPS FOR NITA-U Staff** - NITA-U/SUPLS/19-20/00049
- **ADDENDUM NUMBER I FOR THE SUPPLY**

Thursday, September 26, 2019 - 12:37

Tuesday, September 17, 2019 - 13:03
Primary & Secondary Data Centre Services

The National Data center

In 2012, Cabinet approved the Strategy for Rationalization of Information Technology (IT) Services; with five Strategies, whose objective, among others is to; standardize, streamline and harmonize the acquisition, deployment and disposal of IT services in Government to eliminate duplication; enhance information sharing and interoperability of e-government applications.

In view of this, the Government of Uganda invested in a National Data Centre with a view of centralizing government data centres and minimize the cost of building various Data Centre in MDAs. The National Data Centre is fully equipped with state of the art technology which is utilised for Centralized hosting Services, Disaster Recovery Services and other Data Centre Services for Government Applications & Data.

Currently, NITA-U is providing Data Centre Services which include;

- Platform As A Service (PAAS)
- Infrastructure As A Service (IAAS)
- Software As A Service (SAAS)
- Disaster Recovery AS A Service and Backup AS A Service (BAAS).
Laws, Policies and Regulations

- Computer Use
- Data Security
- Data Protection and Privacy
- Data Backup
- Disaster Recovery Plan
- Data & Information Sharing
Summary

Personnel

Technology

Organisation Policies and Procedures

Laws & Standards

DATA
Acknowledgements

NURTURE Program is funded by Grant Number D43TW010132 supported by:

- Office Of The Director
- National Institutes Of Health (OD)
- National Institute Of Dental & Craniofacial Research (NIDCR)
- National Institute Of Neurological Disorders And Stroke (NINDS), National Heart, Lung, And Blood Institute (NHLBI)
- Fogarty International Center (FIC)
- National Institute On Minority Health And Health Disparities (NIMHD).

Thank You

Questions?
Edward Kakooza
Makerere University College of Health Sciences
ekakooza@chs.mak.ac.ug

Dickson Muyomba
Makerere University College of Health Sciences
dmuyomba@chs.mak.ac.ug