MAKERERE UNIVERSITY BUSINESS SCHOOL

ASSIGNMENT FOR BACHELOR OF COMMERCE

YEAR TWO

SEMESTER ONE

2025

CASE STUDY QUESTIONS

INSTRUCTIONS:

- The cover page must contain name and registration details
- This is individual work
- The work to be hand written and scanned
- To be submitted via wkisaakye@mubs.ac.ug
- Deadline: Friday 22nd/August/2025 at 11:59PM
- It should be typed work with **Times New Romans** font style and font size **12**
- It will contribute to the final examinations' marks

REQUIRED:

Open the links to the data breach case studies to read and answer the following questions below

CASE 1:*https://observer.ug/news/new-study-exposes-data-protection-challenges-in-uganda/*

Case Study: Data Protection Challenges in Uganda - Insights from the 2023 Privacy Scorecard Report

Background:

The 2023 Privacy Scorecard Report released by Unwanted Witness Uganda, a leading digital rights organization, provides a comprehensive evaluation of data protection compliance across several sectors in Uganda. The report assessed 48 companies operating in Uganda, Kenya, Mauritius, and Zimbabwe, focusing on six sectors: telecommunications, financial services, e-commerce, digital services, online betting, and e-government.

Key Findings:

- Limited Public Awareness: There is a low understanding of privacy rights among the general public in Uganda, which increases risks of misuse, breaches, and unauthorized surveillance of personal data.
- Sectoral Performance: Some sectors such as telecoms (notably Lyca Mobile and MTN Uganda) and financial services (Stanbic Bank, Pride Microfinance) scored well on accessibility of privacy policies, with some scoring 100%.
- Significant Challenges: Despite good privacy policy transparency, many sectors including government agencies like DCIC and NIRA performed poorly in critical areas such as:
    - Accountability for data breaches
    - Availability of internal redress mechanisms
    - Data security protocols
    - Managing third-party data transfers

    - Obtaining informed consent from users
- Risk of Data Breaches: Weak data protection practices expose citizens to risks including identity theft, cyberattacks, and unauthorized access to sensitive personal data.
- Case Examples: Notable incidents include hacking of Airtel's mobile money platform where large sums were siphoned off, and users experiencing unauthorized withdrawals due to poor security measures.
- Regulatory and Organizational Gaps: The report highlights insufficient regulatory capacity, resource constraints, weak accountability cultures, and rapid technological changes outpacing compliance efforts.
- Recommendations: Companies and governmental agencies are urged to:
    - Develop transparent, detailed privacy policies covering how data is collected, stored, shared, and protected
    - Implement robust security measures
    - Establish clear mechanisms for reporting and responding to data breaches
    - Improve public awareness of data protection rights and cyber hygiene practices

Case Questions ***(25 marks)***

1. Why is low public awareness of privacy rights a critical issue in the context of data protection in Uganda?
2. What are the main areas where government agencies like DCIC and NIRA are underperforming in terms of data protection? Why are these gaps particularly concerning?
3. How can inadequate accountability and the absence of redress mechanisms after data breaches endanger individuals' personal information?
4. Discuss the impact that weak data protection practices by telecoms and financial services can have on consumers, providing examples from the report.
5. What practical steps can companies and government institutions take to improve compliance with data protection laws and build trust with data subjects?

CASE 2: *https://www.independent.co.ug/cyber-report-reveals-threats-to-ugandan-businesses/*

Case Study: Cybersecurity Threats to Ugandan Businesses in 2024

Background:

In 2024, a survey conducted by Allianz Commercial, an affiliate of Germany-based Allianz Group, revealed that cyber-attacks have become the top business risk for Ugandan executives. This aligns with global trends where cyber incidents like ransomware, data breaches, and IT disruptions have surfaced as the foremost concerns for companies worldwide.

Key Findings:

- In Uganda, 48% of business executives identified cyber incidents as their greatest threat, surpassing concerns such as theft, fraud, corruption, natural disasters, and fire.
- Globally, cyber incidents accounted for 36% of overall risk responses, dominating risk rankings for the third consecutive year.
- Specific cyber threats driving concern include:

    - Data breaches (most worrying for 59% of respondents)
    - Attacks on critical infrastructure and physical assets (53%)
    - Resurgence of ransomware attacks, with insurance claims increasing by over 50% compared to 2022
- Cybercriminals are now leveraging advanced technologies, including generative artificial intelligence (AI), to create more effective malware and phishing attacks.
- A shortage of cybersecurity professionals, especially in Uganda and globally, compounds these risks.

Uganda Specific Context:

- Growing internet coverage and increased digital adoption have expanded the cyber threat surface, many users lacking cyber hygiene awareness.
- The Uganda Police reported 286 cybercrime cases in 2022, resulting in losses exceeding Shs 19.2 billion, yet only a fraction of cases reached conviction or recovery of funds.
- Studies show minimal cybersecurity awareness exists outside core IT teams in both public and private sectors.
- Efforts such as national campaigns ("Be Safe Online") aim to raise public and institutional awareness, but adoption remains inconsistent.
- Cybersecurity is recognized as a shared responsibility among government agencies, businesses, and individuals.

Business Implications:

- Cybersecurity risk is now seen as a threat equal or greater than traditional risks like theft, fraud, or natural disasters.
- Businesses, regardless of size, face similar cyber risks, but smaller firms struggle with resource constraints affecting resilience and recovery.
- Collaboration between organizations and third-party vendors is critical, as risks can propagate through supply chains.
- Companies are urged to prioritize cybersecurity investments, regular risk assessments, and adopt holistic security strategies to protect operations and sensitive data.

Case Questions ***(25 marks)***

1. Why do Ugandan business executives rank cyber-attacks as a higher risk than traditional threats like theft and fraud?
2. What are the main types of cyber threats that concern businesses in Uganda and globally, and how do emerging technologies like AI affect these threats?
3. Discuss the challenges Uganda faces in managing cybercrime effectively, considering the reported cases, convictions, and recovery rates.
4. Explain why cybersecurity is considered a shared responsibility among government, businesses, and individuals in Uganda. How can each stakeholder contribute?
5. What strategies should Ugandan businesses, especially small and medium-sized enterprises (SMEs), adopt to enhance their cybersecurity resilience amid increasing threats?

CASE 3: Court Orders MTN Uganda to Pay for Data Breach

https://redpepper.co.ug/court-orders-mtn-uganda-to-pay-shs-11-3-billion-to-vas-garage-for-data-breach-unfair-practices/139941/

Short Notes:

- Uganda's High Court ordered MTN Uganda to pay Shs.11.3 billion to VAS Garage Ltd for unfair competition and data breach after unlawfully deleting VAS Garage's subscriber database.
- VAS Garage built the database under a licensed agreement, investing significant resources.
- MTN's actions were found to violate the contract and Favor their own mobile content service, which the court deemed anti-competitive.
- The ruling sets precedent for protecting third-party data rights and fair competition against dominant telecom players in Uganda.

Case Questions: ***(20 marks)***

1. What triggered the decade-long legal dispute between MTN Uganda and VAS Garage Ltd?
2. Why did the court rule that MTN's deletion of the database was unlawful and anti-competitive?
3. What key protections for third-party service providers does this ruling reinforce?
4. How does the outcome of this case impact future digital content industry practices and competition in Uganda?

CASE 4: https://eastafricanwatch.net/telecom-giants-mtn-uganda-and-airtel-exposed-breach-of-confidentiality-and-privacy-rights-in-3-56-billion-fraud-case-at-centenary-bank/

Case Study: Breach of Confidentiality and Privacy by MTN Uganda and Airtel in the Centenary Bank Fraud Investigation

Background:

In late 2024, a major privacy scandal emerged in Uganda involving two leading telecommunications firms MTN Uganda and Airtel and Centenary Bank, a prominent financial institution. These telecom companies were implicated in unlawfully disclosing a customer's private data, including call data records (CDRs) and Know Your Customer (KYC) information, to Centenary Bank without proper consent or legal authorization.

Incident Details:

An individual employed at Centenary Bank was accused of involvement in a fraud scheme amounting to 3.56 billion Ugandan shillings. As part of the investigation, MTN Uganda and Airtel provided his call data records to the bank. However, this disclosure was made without a legitimate court order or the data subject's consent, violating Uganda's Communications Act of 2013 and other privacy regulations.

Additionally, Airtel disclosed the victim's KYC data with inaccurate information on location and an incorrect signature. Centenary Bank used this tampered information as evidence to implicate the employee further, resulting in his dismissal.

When the victim sought redress, he found no adequate response from the telecom companies. Upon legal inquiry, Airtel presented a questionable and non-certified court order purportedly authorizing the disclosure. This court order appeared to be irregular, raising concerns about procedural breaches by the police and the misuse of jurisdiction.

Legal and Ethical Issues:

- Breach of Privacy: The telecom companies violated statutory privacy laws protecting customer data.
- Misuse of Data: Call data was shared without proper authorization, and KYC data was falsified.
- Lack of Accountability: Despite complaints, MTN and Airtel failed to properly investigate or respond.
- Potential Abuse of Power: Involvement of law enforcement in issuing questionable court orders suggests institutional weaknesses.
- Impact on Individuals: The victim suffered reputational damage, unjust dismissal, and emotional distress.

Implications:

This incident exposes significant gaps in data protection and corporate governance within both the telecom and banking sectors, highlighting the urgent need for stricter enforcement of privacy laws and transparent protocols governing access to personal data.

Recommendations:

- Regulatory authorities should conduct a thorough investigation and impose sanctions where appropriate.
- Telecom companies must strengthen compliance and internal controls to safeguard customer information.
- Legal frameworks should be revised to clarify and enforce consent and court order requirements.
- Corporations should practice ethical handling of data to prevent misuse and protect individual rights.

Case questions: ***(25 marks)***

1. What legal rights are violated when a telecom company discloses a customer's call data records without consent or a valid court order? How do these rights protect individuals?
2. Explain how falsified Know Your Customer (KYC) information can affect an individual in a fraud investigation. What are the potential consequences of such misinformation?
3. Discuss the responsibilities of telecom companies when handling personal data. What measures should be in place to prevent unauthorized disclosure?
4. Analyse the role of law enforcement in this case, especially regarding the suspicious court order. How does misuse of legal authority impact justice and privacy protection?
5. Suggest key changes that regulators and companies can make to ensure similar breaches of confidentiality do not occur in the future. Consider legal, technical, and ethical aspects.

CASE 5: https://www.watchdoguganda.com/news/20230713/156630/personal-data-protection-office-explains-what-caused-data-security-breach-at-uganda-securities-exchange.html

Case Study: Data Security Breach at Uganda Securities Exchange – Causes and Consequences

Background:

In June 2022, the Uganda Securities Exchange (USE), with support from its technology partner Soft Edge Uganda Limited, experienced a significant data security breach. This breach exposed sensitive personal data of thousands of individuals whose information was collected by USE. The incident prompted an investigation by Uganda's Personal Data Protection Office (PDPO), the national body responsible for enforcing data protection laws.

Incident Details:

The breach resulted from a misconfigured firewall on the audit logging server managed by Soft Edge during an upgrade of USE's Know Your Customer (KYC) system. This error left a port open, allowing unauthorized access to personal data for approximately twelve days before detection.

The compromised data included National Identification Numbers (NINs), names, dates of birth, email addresses, physical addresses, phone numbers, and potentially other sensitive credentials and bank details of investors.

Investigation Findings:

1. Non-compliance with Policies and Laws:
    - Both USE and Soft Edge violated Uganda's Data Protection and Privacy Act, the Information Systems Policies Manual, and related regulations.
    - The change management procedures were not followed during the firewall configuration update.
    - The Maintenance Agreement between USE and Soft Edge lacked crucial data protection and privacy clauses, failing to define the scope and obligations for safeguarding personal data.
2. Lack of Monitoring and Verification:
    - Neither USE nor Soft Edge regularly checked the effectiveness of implemented security safeguards.
    - This negligence allowed the breach to go unnoticed for twelve days, increasing the exposure risk.
3. Legal Registration Oversight:
    - Soft Edge Uganda Limited was not registered with the PDPO as required by law for entities processing personal data, even after the investigation commenced.
4. Recommendations and Enforcement Actions:
    - The PDPO recommended disciplinary proceedings against responsible personnel at USE.
    - USE was urged to implement and enforce comprehensive data protection policies and update agreements with third parties.
    - Enforcement actions were initiated against both USE and Soft Edge for legal violations.

Implications:

The breach exposed personal data to unauthorized parties, undermining investor trust in Uganda's capital markets and raising critical concerns about institutional data governance and cybersecurity resilience.

Lessons Learned:

- Strong adherence to data protection laws and internal policies is vital.

- Effective change management and firewall configuration protocols are essential security practices.
- Regular auditing and timely detection mechanisms can prevent prolonged data exposures.
- Clear contractual obligations between data controllers and processors safeguard personal information.
- Legal registration and compliance of all data processors is mandatory.

Case Questions (25 marks)

1. What are the key responsibilities of organizations like USE and their technology partners in protecting personal data, according to data protection laws?
2. How did the misconfiguration of the firewall contribute to the data breach, and what are the best practices that should have prevented this?
3. Why is it important for data processors such as Soft Edge Uganda Limited to register with the national data protection authority? What risks arise if they do not?
4. Explain how gaps in agreements between data controllers and processors can lead to data protection failures. What should these agreements include?
5. What lessons can other organizations learn from this case to improve their cybersecurity and compliance programs?

END OF TASK