**BIT 4105 - ICT IN BUSINESS IN BUSINESS AND SOCIETY**

**GROUP WORK**

**GROUP MEMBERS;**

1. Allan Cedrick BBIT / 2023 / 40551

2. Robert Kibet BIT / 2023 /40389

3. Mohammed Adan BIT / 2023 / 39770

4. Jecinta Wanjiku BBIT / 2023 / 48178

5. Mercy Gitonga BBIT / 2023 / 50509

6. Joy Wanjiru BBIT / 2023 / 61511

**QUESTION 01**

What sensitive information was exposed in the Business Registration Service (BRS) breach, and who were some of the high-profile individuals affected?

*a) Company Ownership Records:*

* These records include details about who legally owns a business registered in Kenya.
* Ownership records often reveal the stakeholders in a company—both individuals and corporate entities.
* In the breach, these ownership details were compromised, revealing not just names, but potentially identity numbers, addresses, and percentage shareholding.

*b) Directorship Details*

* A director of a company is legally responsible for overseeing the company’s operations and compliance.
* The records exposed could include:
  + Full names of directors
  + National identification numbers
  + Phone numbers, email addresses
  + Board affiliations or other companies they direct

This can expose interlinked business networks and corporate influence structures, making individuals vulnerable to targeted attacks or reputational damage.

*c) Beneficial Ownership Information:*

* A beneficial owner is the true individual who ultimately controls or profits from a business, even if not officially listed in registration documents.
* These details are typically stored for anti-money laundering (AML) and transparency regulations.
* The exposure of such information is particularly dangerous, as it can:
  + Be used for blackmail or extortion
  + Reveal hidden interests of politically exposed persons (PEPs)
  + Undermine business negotiations or financial confidentiality

*High-Profile Individuals Affected:*

The breach specifically impacted politically influential and well-known individuals, making the breach not only a cybersecurity issue but a national political and security concern.

* President William Ruto:
  + As the sitting President of Kenya, any disclosure of his personal or business connections could lead to political vulnerability, national security concerns, and public mistrust.
  + His name being linked to private companies through exposed ownership records adds to the sensitivity.
* The Kenyatta Family:
  + The family of former President Uhuru Kenyatta is known for its vast business empire.
  + Disclosure of their holdings and associations could spark political controversies, potentially unmasking hidden interests or offshore ownership structures.

**QUESTION 02:**

When did the BRS cyberattack occur, and how long did it take for the breach to be reported to the public?

Date of the BRS Cyberattack:

* The cyberattack targeting the Business Registration Service (BRS) occurred during the night of January 31, 2025.
* This means that the attackers likely exploited system vulnerabilities, possibly overnight, when system activity and oversight are lower, increasing the chances of a stealthy intrusion and successful data exfiltration.

Date the Breach Was Reported to the Public:

* The breach was officially reported to the public on February 3, 2025.
* This suggests a time lag of approximately three days between the actual attack and the public disclosure.

**QUESTION 3.**

What actions did the BRS take immediately following the discovery of the breach?

Key Actions Taken by BRS:

*1. Acknowledgement of the Breach*

* The BRS publicly acknowledged the incident shortly after it occurred, issuing a statement by February 3, 2025.
* This early admission was important for transparency, especially since the breach involved high-profile individuals like President William Ruto and members of the Kenyatta family.
* The statement confirmed that sensitive data had been accessed but did not go into full technical details, likely due to the ongoing investigation.

*2. Strengthening of Security Protocols*

* The Director General of BRS, Kenneth Gathuma, announced that the agency had immediately strengthened its cybersecurity protocols.
* While the specific upgrades were not detailed, this likely included:
* Patching known vulnerabilities
* Updating firewalls and antivirus systems
* Increasing monitoring of network activity
* Resetting access credentials, especially for employees and administrators

*3. Launch of a Formal Investigation*

* BRS launched a comprehensive internal and external investigation into the breach.
* This included collaboration with:
* Cybersecurity experts to analyse how the breach occurred and how much data was compromised.
* Law enforcement agencies to trace the perpetrators, understand the legal implications, and build a criminal case if needed.
* Investigators likely focused on:
* Identifying whether the breach came through phishing, credential theft, or system vulnerabilities
* Understanding the attack path (how the intruder moved through the system)
* Assessing what data was accessed, copied, or exfiltrated

*4. Commitment to Transparency*

* BRS made a public commitment to maintain transparency during the investigation.
* This was intended to rebuild trust among the Kenyan public, private businesses, and government stakeholders.
* However, the lack of detailed information about the root cause, methods used by attackers, and extent of damage led to some public scepticism and concerns about accountability.

**QUESTION 4.**

Analyse the potential consequences of the BRS breach for the privacy and security of the affected high-profile individuals and businesses.

The breach at Kenya’s Business Registration Service (BRS) had serious privacy and security implications, especially given the sensitive nature of the data involved. Because BRS manages the official records of business ownership, directorship, and beneficial ownership, the data leak could have far-reaching consequences for individuals, companies, and even the country’s governance and economy.

*Types of Data Exposed*

The breach compromised:

1. Company Ownership Records
   * Details about who legally owns specific companies.
   * This includes names, ID numbers, and equity stakes.
2. Directorship Information
   * Names and personal information of directors, often used to map business networks.
3. Beneficial Owner Information
   * People who *ultimately control or benefit from* a company’s profits, even if not publicly listed.
   * This is especially sensitive in cases of shell companies or politically exposed persons (PEPs).

Who Was Affected?

The breach affected high-profile individuals, including:

* President William Ruto
* Members of the Kenyatta family
* Other business elites and potentially foreign investors connected to Kenya-registered companies.

Privacy and Security Consequences

*1. Loss of Confidentiality and Personal Privacy*

* Exposed personal details can be used to:
  + Track financial interests
  + Target individuals for surveillance or extortion
* For political leaders, this is especially dangerous and could expose conflicts of interest, hidden wealth, or offshore holdings.

2. Targeted Social Engineering and Phishing Attacks

* Attackers can craft highly personalized phishing emails or impersonation attacks using the leaked information.
* A director’s contact details can be used to trick staff or partners into transferring money or confidential documents.

*3. Reputational Damage*

* Being linked to controversial business arrangements, hidden assets, or certain directors could damage:
  + Public image
  + Political careers
  + Investor confidence

*4. Financial Fraud and Identity Theft*

* Attackers can:
  + Open fake accounts or businesses in someone’s name
  + Steal money via social engineering or fake transactions
  + Forge ownership documents

*5. Legal and Regulatory Risks*

* Companies and individuals may face scrutiny from:
  + Anti-corruption bodies
  + Tax authorities
  + International regulators (e.g., in money laundering investigations)

*6. Business Disruption*

* Public or private organizations may face:
  + Loss of clients due to perceived insecurity
  + Audits and investigations
  + Reduced foreign investment if Kenya is seen as unsafe for business data

*7. Political Ramifications*

* Data linking politicians to hidden companies or networks may fuel:
  + Public distrust
  + Opposition criticism
  + Political instability, especially if timed near elections or policy decisions

**QUESTION 5.**

Compare the BRS breach with the 2023 eCitizen platform cyberattack in terms of their impact on public trust in Kenyan government systems.

| Aspect | BRS Breach (2025) | eCitizen Attack (2023) |
| --- | --- | --- |
| Nature of Data | Ownership, directorships | Service disruption, not direct data theft |
| High-Profile Involvement | Yes – Ruto, Kenyatta’s | No specific individuals identified |
| System Function | Company registry | Government service portal |
| Impact on Trust | Damaging due to exposure of elites | Disruptive but temporary |
| Public Response | Increased concern over data security | Frustration due to access issues |

Comparison of Public Trust Impact

*1. Nature of the Breach*

* BRS: The breach exposed highly sensitive and confidential ownership records, which could be misused for identity theft, fraud, or political manipulation. This creates fear around how well the government protects private information.
* eCitizen: Although no data was stolen, the attack caused widespread service outages, affecting millions who rely on the platform for daily transactions like passport renewals, business licenses, and birth certificate applications.

Impact:

* BRS: Erodes confidence in data security and internal systems.
* eCitizen: Damages perception of government reliability and digital preparedness.

*2. Target Audience Affected*

* BRS: Mainly affected elites, businesspeople, and politically exposed persons.
* eCitizen: Affected everyday citizens, including students, business owners, and families who rely on timely access to services.

Impact:

* BRS: Public sees government systems as biased or insecure.
* eCitizen: Citizens feel frustrated, possibly digitally excluded, especially in rural areas with limited alternatives.

*3. Political and Institutional Trust*

* The BRS breach struck at the heart of transparency and anti-corruption efforts. If high-profile individuals’ data is leaked, and no accountability follows, citizens may feel that government officials are above the law or that the system is politically compromised.
* The eCitizen attack, by contrast, suggests a lack of technical resilience and disaster preparedness. It raises doubts about whether Kenya is ready to handle full digital transformation.

Impact:

* BRS: Creates distrust in integrity and fairness of government data handling.
* eCitizen: Undermines faith in service continuity and uptime guarantees.

*4. Government Response and Communication*

* BRS: Response was vague. While the agency admitted the breach, it did not explain the technical root cause or the full extent of the damage. This lack of transparency raised concerns about a cover-up.
* eCitizen: The government publicly acknowledged the DDoS attack and worked to restore services. Although details were limited, the communication was relatively prompt.

Impact:

* BRS: Perceived lack of accountability damages public trust more deeply.
* eCitizen: Communication slightly cushioned the trust blow, though not completely.

*5. Overall Impact on Public Trust*

* Short-Term Trust Impact:
  + BRS breach: Citizens, journalists, and watchdogs questioned the ethical handling of sensitive data and potential for abuse.
  + eCitizen attack: People lost faith in the government’s technical competence.
* Long-Term Trust Impact:
  + BRS: Undermines public belief in data privacy, deters business registrations, and possibly affects foreign investment.
  + eCitizen: Highlights the fragility of Kenya’s digital public services, risking pushback against future digitization efforts.

**QUESTION 6.**

Evaluate the BRS’s response to the breach—how effective was their approach in addressing public concerns and preventing future incidents?

The Business Registration Service (BRS) breach in early 2025 was a critical event that exposed significant weaknesses in cybersecurity governance within a key Kenyan government agency. The effectiveness of the BRS's response to this breach can be evaluated across several key dimensions: acknowledgment and communication, technical investigation, preventive actions, and public confidence restoration.

*1. Acknowledgment and Public Communication*

What BRS Did:

* BRS Director General Kenneth Gathuma publicly acknowledged the breach shortly after it was reported (on February 3, 2025).
* The agency announced it was strengthening security protocols and committed to transparency.

Evaluation:

* While prompt acknowledgment is commendable, the lack of specific details on how the breach occurred or who was responsible created uncertainty and speculation.
* BRS did not disclose the exact number of records accessed, the technical vulnerability exploited, or the timeframe in which systems were compromised.
* This vagueness weakened public confidence, as citizens and businesses were left unsure about whether their data had been compromised and how it might be misused.

Effectiveness Rating: *Moderate*  
Explanation: The public statement showed willingness to admit the issue, but limited transparency undermined its credibility.

*2. Technical Investigation and Forensics*

What BRS Did:

* BRS engaged cybersecurity experts and law enforcement agencies to investigate the incident.
* It was implied that internal reviews and system audits were initiated.

Evaluation:

* However, no public technical report or executive summary of findings has been released (as of available reporting).
* Without technical disclosure, the root cause remains unclear—was it phishing, a misconfiguration, insider threat, or a known exploit?
* A lack of clarity reduces public and stakeholder trust and prevents other agencies or private entities from learning preventive lessons.

Effectiveness Rating: *Low to Moderate*  
Explanation: Initiating investigations is necessary, but failure to share findings limits learning and public reassurance.

*3. Strengthening Cybersecurity Protocols*

What BRS Claimed:

* BRS announced it had improved internal cybersecurity controls after the breach.

Evaluation:

* The agency did not provide concrete examples of what measures were implemented:
  + Were new firewalls or intrusion detection systems (IDS) installed?
  + Were systems patched or software updated?
  + Was employee training improved?
* Without specifics, the claim of “strengthened protocols” feels more like damage control than a strategic reform.
* This also missed the opportunity to set a positive precedent for other government institutions facing similar risks.

Effectiveness Rating: *Low*  
Explanation: Vague improvements do little to restore trust or show actual readiness for future attacks.

*4. Addressing Public Concerns and Accountability*

What the Public Needed:

* Citizens and businesses wanted:
  + A clear account of who was affected
  + A timeline of the breach and response
  + Assurance that their data would be protected in the future

What Was Delivered:

* BRS did not provide individual notifications to affected companies or individuals.
* There was no mention of support services like credit monitoring, breach notification letters, or a helpdesk for concerned businesses.
* No officials were held publicly accountable, and no internal policy changes were made public.

Effectiveness Rating: *Very Low*  
Explanation: The response failed to directly engage with the public, provide support or clarity, or show institutional accountability.

Overall Assessment

The BRS’s response was partially effective but largely insufficient in addressing public concerns and restoring trust:

* Strengths: Immediate acknowledgment and involvement of cybersecurity professionals.
* Weaknesses:
  + Lack of transparency
  + No detailed incident disclosure
  + No direct communication with affected parties
  + No visible policy changes or employee training response

This inadequate response likely deepened public scepticism about the Kenyan government's ability to manage and protect sensitive digital infrastructure. It also signalled a lack of preparedness, especially for incidents involving high-profile individuals, potentially undermining both business confidence and digital transformation efforts.

Overall Effectiveness: Moderate. While BRS took standard response steps, they failed to rebuild public trust through detailed disclosures or public outreach.

**QUESTION 7.**

If you were a cybersecurity advisor for the BRS, what specific measures would you recommend to prevent similar breaches in the future, considering Kenya’s high cyberattack rate?

As a cybersecurity advisor to the Business Registration Service (BRS), my recommendations would focus on a multi-layered cybersecurity strategy that addresses both technical infrastructure and human vulnerabilities, especially given Kenya’s high rate of cyberattacks (860 million in the past year).

*1. Conduct a Comprehensive Security Audit*

* Why? To identify all current vulnerabilities—misconfigured servers, outdated software, weak authentication mechanisms, etc.
* Action: Partner with certified cybersecurity firms to conduct penetration testing and vulnerability scans.
* Outcome: A prioritized list of weaknesses and a roadmap for remediation.

*2. Implement Multi-Factor Authentication (MFA)*

* Why? Passwords alone are not enough; MFA adds an additional layer of protection (e.g., OTPs, biometrics).
* Action: Mandate MFA for all employee and administrative logins, especially those accessing sensitive records.

*3. Encrypt Sensitive Data at Rest and in Transit*

* Why? Even if attackers gain access, encrypted data will be unreadable without the decryption keys.
* Action: Use AES-256 encryption for databases and SSL/TLS for data transmitted over networks.
* Outcome: Minimized risk of data theft and tampering.

*4. Patch Management System*

* Why? Many breaches exploit outdated software with known vulnerabilities.
* Action: Automate the detection and deployment of patches for operating systems, database software, and third-party tools.

*5. Deploy Advanced Threat Detection Tools*

* Why? To monitor for unusual activity, such as large data exports or login attempts from unknown IPs.
* Tools: SIEM (Security Information and Event Management), Intrusion Detection Systems (IDS), and endpoint monitoring.
* Outcome: Real-time alerts to stop breaches in progress.

*6. Mandatory Cybersecurity Awareness Training*

* Why? Many breaches, including the suspected BRS one, begin with phishing or human error.
* Action: Quarterly training on:
  + Recognizing phishing emails
  + Using strong passwords
  + Reporting suspicious activities
* Outcome: A workforce that acts as the first line of defences, not a vulnerability.

*7. Internal Access Controls (Principle of Least Privilege)*

* Why? Not every employee needs access to all data.
* Action: Restrict access based on role, with auditing to ensure no unauthorized data access.
* Example: Only a handful of vetted personnel should be able to view beneficial ownership data.

*8. Incident Response Plan (IRP)*

* Why? In case of future breaches, fast and effective response minimizes damage.
* Contents:
  + Communication plan
  + Roles/responsibilities
  + Steps for containment, eradication, and recovery
* Outcome: Reduced chaos and quicker mitigation during incidents.

*9. Create a Cybersecurity Governance Board*

* Why? Oversight ensures that cybersecurity remains a priority, not an afterthought.
* Composition: Mix of IT staff, legal advisors, executive leadership, and an external cybersecurity consultant.
* Duties: Policy reviews, breach simulations, budget reviews.

*10. Implement a Public Breach Notification Protocol*

* Why? Transparency builds trust.
* Action: Establish clear guidelines for:
  + When the public must be notified
  + How affected individuals will be contacted
  + Support services (e.g., credit monitoring)
* Outcome: Increased public confidence and reduced backlash.

**QUESTION 8.**

Design a 4-step employee training program for Kenyan government agencies like the BRS to reduce the risk of phishing attacks.

The Business Registration Service (BRS) cyberattack likely stemmed from a phishing or spear phishing attempt, a method commonly used to trick employees into granting attackers access. A structured employee training program is essential to reduce this risk, especially in government agencies where sensitive citizen and corporate data is stored.

Below is a detailed 4-step training program specifically tailored for Kenyan government agencies, including the BRS:

*Step 1: Awareness & Education Workshops*

Objective: Build foundational knowledge of cyber threats, with a strong focus on phishing.

Content:

* What is phishing, spear phishing, and social engineering?
* Real-life examples from Kenyan and global government breaches (e.g., BRS, eCitizen, Equifax).
* Types of phishing: email, SMS (smishing), voice calls (vishing), social media.

Format:

* Monthly in-person or virtual workshops.
* Interactive simulations showing real vs. fake emails.
* Case study: The January 2025 BRS breach—how phishing might have played a role.

Outcome: Employees can recognize suspicious messages and understand the real-world stakes of data breaches.

*Step 2: Simulated Phishing Campaigns*

Objective: Test how employees respond to realistic phishing attempts.

Content:

* Send fake but realistic phishing emails (e.g., fake password reset requests or fake internal memos).
* Monitor who clicks links, submits credentials, or reports the email.

Format:

* Quarterly simulations across all departments.
* Vary the complexity and types of attacks.

Response Plan:

* If an employee fails a simulation, they are enrolled in immediate follow-up micro training.
* Publicly reward correct responses (e.g., reporting a phish) to promote a culture of vigilance.

Outcome: Improves real-time recognition skills and highlights weak spots in the workforce.

*Step 3: Secure Behaviour Reinforcement*

Objective: Encourage secure habits and reduce reliance on memory alone.

Focus Areas:

* Always verify senders of emails requesting sensitive actions.
* Never download attachments or click links from unknown sources.
* Use strong, unique passwords and never reuse them.
* Enable and understand two-factor authentication (2FA).

Tools & Materials:

* Posters in offices and intranets: “Think Before You Click”
* Email reminders: “Phishing Tip of the Week”
* Cyber hygiene checklists for all employees

Outcome: Promotes secure-by-default behaviour and makes caution a daily habit.

*Step 4: Incident Reporting & Response Training*

Objective: Ensure employees know how to respond to and report phishing attempts quickly.

Topics:

* How to report a suspected phishing email (e.g., to the IT security team or a dedicated email like phishing@brs.go.ke)
* What to do if you accidentally click a suspicious link or share credentials
* Role-playing exercises to practice reporting

Tools: Dedicated hotline or ticket system for cybersecurity incidents.

Outcome:

Ensures rapid containment of threats and turns employees into active defenders, not passive users.

Summary of the 4-Step Phishing Prevention Program

| Step | Title | Key Focus | Frequency |
| --- | --- | --- | --- |
| 1 | Awareness & Education Workshops | What phishing is and why it matters | Monthly |
| 2 | Simulated Phishing Campaigns | Practice recognizing and reporting attacks | Quarterly |
| 3 | Secure Behaviour Reinforcement | Promote everyday cyber hygiene | Ongoing |
| 4 | Reporting & Response Training | What to do when phishing is suspected | Biannually |

Had the BRS implemented a program like this before January 2025, it could have reduced the risk of phishing-based intrusions. Trained employees are far less likely to fall victim to social engineering, and when they do, they’re more likely to respond appropriately and quickly, minimizing damage.

**QUESTION 9**

Propose a strategy for a Kenyan SME to protect its business registration data when interacting with government agencies like the BRS, given the recent breach.

SME Data Protection Strategy:

*Step 1: Minimize Data Exposure During Transactions*

Action: Only submit mandatory data required by government agencies. Avoid oversharing non- essential documents or company records.

How:

* Review official forms and only fill in required fields.
* Avoid emailing sensitive company documents—use official portals or in-person submissions where safer.
* Use data redaction (e.g., blur out unrelated information) when sharing scanned ID documents or shareholder details.

Goal: Reduce the amount of sensitive data that could be exposed in a future breach.

*Step 2: Use Secure Communication Channels*

Action: Always use secure websites (HTTPS), encrypted portals, or official government channels for submission and inquiries.

How:

* When interacting with the BRS online, ensure the URL starts with https://brs.ecitizen.go.ke.
* Avoid submitting any information via personal email addresses or unofficial WhatsApp groups.
* Confirm legitimacy of communication—verify sender emails or messages via the BRS helpline.

Goal: Prevent data interception or man-in-the-middle attacks during transmission.

*Step 3: Conduct Periodic Risk Assessments and Vendor Vetting*

Action: Regularly assess your SME's exposure and data practices when dealing with third parties or government contractors.

How:

* Ask: Who stores or processes our business registration data?
* Confirm that consultants or third-party agents (if used) follow strict data protection measures.
* Sign Non-Disclosure Agreements (NDAs) with consultants or lawyers who help with business registration.

Goal: Ensure your data isn't compromised by careless intermediaries.

*Step 4: Implement Data Backup & Encryption Policies*

Action: Backup all sensitive registration data in a secure, encrypted form before uploading or submitting to any government platform.

How:

* Store encrypted copies of business documents on cloud platforms with two-factor authentication (e.g., Google Drive with encryption tools).
* Use PDF password protection or document encryption software (e.g., VeraCrypt, BitLocker).
* Label documents clearly with version and access restrictions (e.g., "Confidential – BRS use only").

Goal: Even if a breach occurs, your original data remains uncompromised and recoverable.

*Step 5: Monitor Public Records and Audit Trails*

Action: Frequently check government portals for your company’s public-facing records to ensure no unauthorized changes were made.

How:

* Visit the BRS online portal monthly to verify ownership and directorship data.
* Enable notifications (if supported) for updates to your business profile.
* Track who within your SME accesses sensitive documents—maintain an internal audit trail.

Goal: Detect data tampering early and respond before damage escalates.

*Step 6: Advocate for Transparency & Accountability*

Action: Hold agencies like BRS accountable for protecting your data.

How:

* If your SME is part of a chamber of commerce or trade group, advocate for stronger data protection policies.
* Request written data handling practices from BRS or government partners before sharing sensitive files.
* Encourage whistleblowing on suspicious or corrupt practices related to company records.

Goal: Push for systemic cybersecurity reforms and protect SMEs collectively.

**QUESTION 10**

Reflect on the role of employee training in preventing data breaches—how could better training have potentially mitigated the BRS incident?

*Overview: Why Employee Training Matters in Cybersecurity*

In cybersecurity, human error is one of the weakest links. Many high-profile data breaches worldwide — including the Business Registration Service (BRS) breach in Kenya — have either started with or been exacerbated by employee mistakes, such as clicking on phishing emails, using weak passwords, or failing to follow protocol. The BRS breach, suspected to have been initiated through spear phishing, highlights just how critical proper employee training is in safeguarding sensitive government data.

Employee cybersecurity training involves teaching staff at all levels:

* How to identify and avoid cyber threats
* How to secure data and systems
* How to respond appropriately to security incidents
* How to comply with policies, legal standards, and best practices

*Role of Employee Training in Preventing the BRS Breach*

1. Spear phishing Awareness & Email Hygiene

What likely happened:  
Reports suggest that the BRS breach may have begun when an employee opened a spear phishing email — a highly targeted attack that tricks users into opening malicious links or files.

With proper training:

* Employees would be trained to identify suspicious emails, especially those with urgent requests, unusual links, or attachments.
* Training would cover how to verify sender addresses and avoid clicking on unfamiliar content.
* They would be instructed to report suspicious messages immediately to IT/security teams.

Impact: The initial attack vector could have been blocked if the employee recognized and avoided the phishing email.

2. Secure Use of Devices & Software

What likely happened:  
If attackers exploited a system vulnerability or gained access to login credentials, they may have moved laterally through the network.

With proper training:

* Staff would understand the importance of strong passwords, 2FA (two-factor authentication), and device security.
* They would be discouraged from reusing passwords, sharing credentials, or storing sensitive info in unprotected documents.
* Training would include logging off systems and reporting stolen/lost devices promptly.

Impact: Even if a phishing attempt succeeded, access might have been limited by stronger internal security practices.

3. Incident Detection & Response Training

What likely happened:  
After the breach began, there may have been delays in identifying and containing the intrusion.With proper training:

* Staff would be trained to recognize signs of system compromise (e.g., unusual system behaviour or access logs).
* Clear protocols would guide them to report incidents swiftly to the IT department.
* Regular incident response drills would ensure quick, coordinated action.

Impact: Quicker detection could have minimized the data exposed and reduced reputational damage.

4. Compliance & Responsibility Culture

What likely happened: There may have been weak enforcement of security policies or a lack of accountability regarding data handling.

With proper training:

* Employees would understand the legal and ethical implications of data protection failures.
* Regular refreshers would reinforce a culture of security — making cybersecurity a daily priority, not a one-time topic.
* Leaders would model good practices and ensure all staff comply with protocols.

Impact: A well-informed, vigilant workforce would be more likely to follow procedures that prevent breaches.