KPMG

Privacy Digest

Issue 1 | March 2024 | KPMG in Nigeria

Data Breaches: Insights and Lessons

In this edition, we focus on data breaches, revealing lessons from real-life case studies, practical strategies for mitigating them, and the position of the data protection law on managing data breaches.

While organisations diligently implement controls to mitigate cyberattacks, the persistent occurrence of data breaches is still a challenging reality. Despite technological advancements, data breaches continue to occur, emphasizing that technology alone cannot entirely eradicate these incidents. The root cause often extends beyond technical vulnerabilities, revealing that some breaches stem from human-based errors.

Globally, regulators across different jurisdictions such as the European Data Protection Supervisor (EDPS) of Europe, the Nigeria Data Protection Commission (NDPC) of Nigeria, and the Information Commissioner's Office (ICO) of the United Kingdom have documented the definition of what constitutes a personal data breach within their respective data protection laws/regulations. In the Nigeria Data Protection Act (NDPA), a personal data breach is defined as a breach of security of a data controller or data processor **leading to, or likely to lead to**, the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
This bulletin delves into comprehensive case studies of data breach incidents, examines potential data breach scenarios and their treatment, and discusses the regulatory requirements in handling data breaches including responsibilities that organisations need to be aware of.

Data Breach Case Studies

The relationship between data security and data privacy is evident, as the lack of adequate data security measures can leave organisations vulnerable to penalties, particularly when there is a personal data breach. Globally, regulatory bodies have imposed fines on organisations for a range of infractions, including inadequate lawful basis for processing personal data, failure to comply with general data processing principles, insufficient implementation of technical and organizational safeguards for information security, and failure to cooperate with supervisory authorities in cases of breaches.

According to the GDPR Enforcement Tracker from July 2018 to March 2024, various organisations have been fined a sum of €391,263,875 for insufficient technical and organizational measures to ensure information security and a sum of €2,675,582 for insufficient fulfilment of data breach notification obligations.
Examining real-world case studies provides valuable insights into the diverse factors and vulnerabilities contributing to these incidents. Through the lens of actual events, we can gain lessons and strategies to fortify our defences against cyber threats.

Case Study 1

[1]In 2020, the Information Commissioner's Office (ICO) levied a £20 million ($26 million) fine against British Airways (BA) for a breach that compromised both personal and credit card data of over 400,000 customers in 2018. Attackers infiltrated BA's systems and modified them to harvest customer details. The breach went unnoticed for two months until a security researcher discovered it and alerted BA, prompting the subsequent notification to the ICO. [2]BA revealed that hackers successfully breached its website and app, resulting in the theft of data from numerous customers. The stolen data included login credentials, payment card information, travel booking details, as well as personal details like names and addresses. An investigation concluded that adequate security measures, such as multi-factor authentication, were not in place at the time of the breach. While BA did not disclose specific technical details about the breach, cybersecurity experts suggest that a malicious code embedded within the BA website or app could have surreptitiously collected and transmitted customer details to an unauthorized party while they entered their details on the system. Other, security experts suggested that the breach might have happened through an integration with a compromised third-party payment gateway provider.

Key observations from Case Study 1

- The breach being active for an extended period without detection is an indication that there may have been no proper security monitoring in place on the BA's website or the Mobile App at the time of the breach.
- Certain security controls such as MFA which should have been enabled were not enabled at the time. Hence, BA may not have optimized security measures at its disposal at the time which might have contributed to the success of the attack.

[1]British Airways fined £20m over data breach
[2]British Airways breach: How did hackers get in?

Real-Life Data Breach Case Studies (Contd.)

Recommendation for organisations

- There is a need to establish a clear process for performing regular audits to assess the adequacy of security controls on web and mobile applications.
- Organisations need to implement real-time security monitoring capabilities to adequately detect unusual activities around key systems.
- There is a need for organisations to optimize security features on solutions already implemented to maximise capabilities and ROI on security spend.

Case Study 2

[3]In September 2022, Uber discovered its computer network had been breached, leading to a temporary shutdown of several internal communications and engineering systems. During the investigation, it was revealed that a hacker purchased stolen credentials of an employee from a dark web marketplace. However, an initial attempt by the hacker to connect to the Uber network with these credentials failed because the account was protected with Multi-Factor Authentication (MFA). [4]To overcome this security obstacle, the hacker contacted the employee via WhatsApp, posing as a member of Uber's security team, and pressured him to approve MFA notifications sent to his phone. [5]The employee became overwhelmed by the flood of notifications messages claiming to be from Uber's IT department instructing the employee to confirm that the login attempt was legitimate, and he eventually approved the request, granting the hacker network access via the VPN, the hacker uncovered Microsoft PowerShell scripts that contained the login credentials of an admin user in Uber's Privileged Access Management (PAM) solution. This finding escalated the severity of the breach, providing the intruder with complete administrative access to all of Uber's sensitive services, such as DA, DUO, Onelogin, Amazon Web Services (AWS), and GSuite.

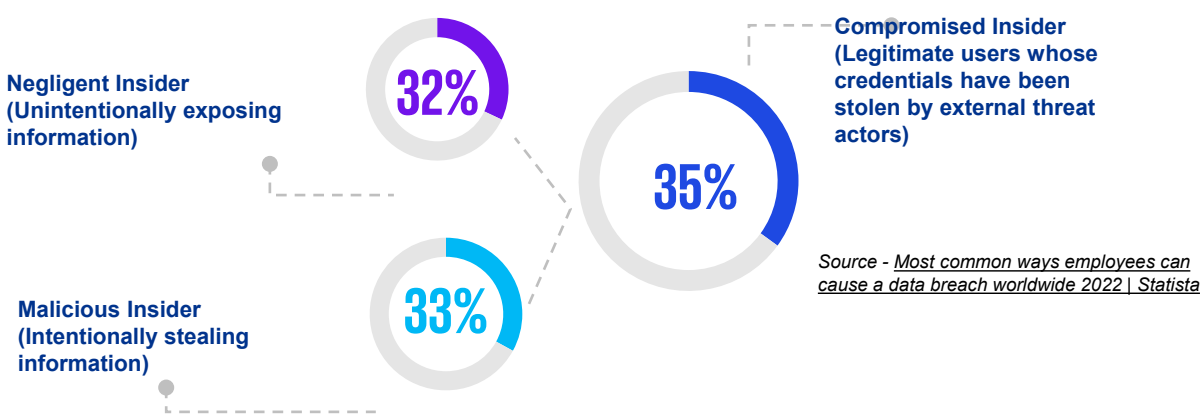
Key Observations from Case Study 2

- The hacker was able to deploy various attack techniques at every stage of its journey. First, we noted that stolen credentials were available to initiate authentication attempts to Uber's VPN service. In addition, the MFA which posed an initial roadblock was surmounted via a social engineering attack. Subsequently, the attacker was able to escalate privileges by gaining access to a clear text admin password, which led to unauthorized access to several databases and rendered some systems inaccessible.
- Despite the MFA and possibly other layers of security, humans appear to still be the weakest link, and this was exploited in the security breach.
- The practice of having application and service account credentials stored in scripts is a common practice across many organisations and in the case of Uber, there were admin credentials in a PowerShell script which opened up an opportunity for the hacker to gain unauthorised access to many other systems.
- The fact that the employee login credentials were available on the dark web over an extended period without the knowledge of Uber shows the need for cyber threat intelligence capabilities.

Recommendation for organisations

- There is a need to ensure secure coding practices are adhered to, such that clear text login details are not left in scripts, as this can easily be exploited by unauthorized users.
- Information Security teams need to understand the tactics of attackers as an input in enriching end-user cyber security awareness training programmes.
- Given the sophistication of cyber-attack syndicate activities within the dark web, it is important that organisations deploy cyber threat intelligence capabilities that would proactively scan and give insight into their level of exposure on the dark web. This would enable organisations to take preventive measures to proactively remediate any gaps before they are exploited.

From the case study, despite the organization's best efforts, employees remain the weakest link in the data breach chain. A recent research conducted highlights the most common ways employees contribute to data breaches in worldwide organisations from March 2022 to March 2023.



Source - Most common ways employees can cause a data breach worldwide 2022 | Statista

[3]*Uber Hack Update*
[4]*Uber Investigating Breach of Its Computer Systems*
[5]*What Caused the Uber Data Breach in 2022? | UpGuard*

What Would You Classify as a Data Breach?

Below, we will explore various scenarios related to data breaches, delving into the reasons behind classifying them as either data breaches or non-incidents.

S/N	Scenario	Indication of a potential data breach?	Why?/Why not?
1	The company conducts a simulated phishing exercise to test employees' awareness. Employees receive fake phishing emails to see if they can identify and report them.	No	No, this is not a data breach. The simulated phishing exercise is a proactive measure to enhance employees' awareness of potential threats. It is a controlled and planned activity conducted for educational purposes.
2	An employee loses their company-issued laptop. The laptop contains sensitive customer information, but it's password-protected.	Yes	This is a potential data breach. While the laptop may be password-protected, the sensitivity of the data it contains poses a risk. If the password is compromised or the data is accessed, it could lead to unauthorized disclosure.
3	An employee notices that someone accessed their computer without permission over the weekend. No files seem to be missing, but the login history shows unauthorized access.	Yes	Yes, this is a data breach. Unauthorized access indicates a security incident, even if no files are missing. The fact that someone gained unauthorized access is a breach of security.
4	The IT department schedules routine system maintenance during non-business hours. Some employees notice temporary disruptions in accessing files during this time.	No	No, this is not a data breach. Routine system maintenance is a planned activity aimed at keeping systems secure and up-to-date. Temporary disruptions during maintenance are expected and do not compromise data integrity.
5	IT administrators detect a significant increase in outbound network traffic during non-business hours. It is unclear whether the traffic is legitimate, or it indicates unauthorized data exfiltration.	Yes	Yes, the unusual outbound network traffic may signal a potential data breach. Investigating the nature of the traffic and determining if it aligns with normal business activities is crucial. It could be indicative of data exfiltration.
6	An HR personnel mistakenly sends an Excel sheet containing employee payroll data to the wrong recipient.	Yes	Yes, this is a data breach caused by the unauthorized disclosure of personal data transmitted. While dealing with a wrong recipient within the organization may be easier to manage, outside the organization will likely cause serious issues.

How Compliant Are You in Managing Data Breaches?

The NDPA has established regulatory requirements for organisations known as data controllers, outlining their responsibilities in the event of a data breach. In recent times, organisations often outsource processes to third-party entities. These third-party entities, known as data processors, also bear responsibilities in the event of a data breach.

Section 40 (1), (2), and (3) of the NDPA instructs that if a breach is identified, immediate notification to the engaging data controller is required, providing details of the breach and responding promptly to information requests to meet regulatory obligations. The data controller, within 72 hours of identifying a breach **posing a risk to individuals' rights**, must inform the Commission. If the breach is likely to significantly impact a data subject, the data controller must communicate the breach promptly, offering guidance in clear language. If direct communication poses challenges, a public announcement may be made through widely used media sources.

Section 48 (3), (4), and (5) of the NDPA specifies that a penalty or remedial fee for a data breach may vary based on the importance of the data controller or data processor. For those of major importance, the penalty may be up to the greater of N10,000,000 or 2% of the annual gross revenue in the preceding financial year. For those not of major importance, the penalty may be up to the greater of N2,000,000 or 2% of the annual gross revenue in the preceding financial year.

We would love to have your take

1. What is the most challenging part of managing data breaches and why?
2. In your own opinion, why do organisations hesitate to report data breaches to the regulatory authority?
3. Which of the four (4) instances of potential data breaches above will you be hesitant to report to the NDPC and/or data subjects?

*W*e would love to hear from you. Kindly provide feedback via https://forms.office.com/e/s1qdPzQUzs

For further information, contact:

John Anyanwu
Partner, Cyber & Privacy
KPMG Nigeria
T: +234 803 975 4061
Email: john.anyanwu@ng.kpmg.com

Olaoluwa Agbaje
Senior Manager, Cyber and Privacy
KPMG Nigeria
T: +234 816 960 8200
Email: Olaoluwa.Agbaje@ng.kpmg.com

Contributors

Kudirat Tobi Mustapha

Obehi Emiowele

Muiz Adeleke

Glory Obi

kpmg.com/socialmedia
kpmg.com/app

Download on the App Store