E-BULETIN
EDISI
2023

UNIVERSITI TEKNOLOGI MARA
Cawangan Negeri Sembilan
Kampus Rembau

RONA TINTA

e-BULETIN 2023

FAKULTI PENGURUSAN & PERNIAGAAN

UNIVERSITI TEKNOLOGI MARA
CAWANGAN NEGERI SEMBILAN
KAMPUS REMBAU

DATA BREACH: CAUSES, IMPLICATIONS, AND LESSON LEARNED

Mohd Faizal Mohd Ramsi, Sufy Rabea Adawiya Idris & Siti Khairiyah Nordin

Pengajian Sains Maklumat, KPPIM

UiTM Cawangan Negeri Sembilan Kampus Rembau

Data and information are crucial assets. Some of the administrators treat data and information as crucial business tools no matter their size, their industry, or their technical competencies. Data breaches pose a significant threat to organisations because they can lead to compromised sensitive information and undermine trust. Recent data leak incident at one of Malaysia's leading universities had a huge impact on the academic institution, its customers, staff, and its stakeholders. The incident involved unauthorised access to its databases containing personal and academic information of students, faculty, and staff. The breach caused concern as it potentially exposed sensitive data, including names, identification numbers, contact details, and academic records. Unfortunately, it had attracted media attention and raised concerns about the university's data security practices.

Data Breach: Causes

A data breach, also known as data exposure, refers to the unauthorised or accidental release of sensitive or confidential information from a secure location to an unsecured environment. It occurs when sensitive data is accessed, disclosed, or distributed without proper authorization, potentially exposing it to unauthorised individuals or entities. It can occur in various ways, namely:

- Hacking: Cybercriminals gain unauthorised access to a system or network and extract sensitive data.
- Insider threats: Employees or individuals with legitimate access intentionally or unintentionally expose confidential information.
- Lost or stolen devices: Misplaced or stolen laptops, smartphones, or storage devices containing sensitive data can result in a data leak.
- Malware or viruses: Malicious software can infiltrate a system and extract data without the user's knowledge.
- Social engineering: Manipulating individuals into revealing sensitive information, such as through phishing attacks or impersonation.

- Weak security practices: Inadequate security measures, such as weak passwords, use of not genuine software, or reconfiguration of systems can make data more vulnerable to leaks.

Data Breach: Implications

Additionally, the impact of a data breach can be far-reaching and have serious consequences for individuals and especially organisations, which can affect their reputation and trustworthiness. The compromised personal information could be exploited for identity theft, fraud, or targeted phishing attacks. Data breach can damage the trust between an institution and its stakeholders. In the recent incident, affected students, faculty, and staff may question the university's commitment to protecting their personal information. A loss of trust can have long-term implications for student enrollment, faculty retention, and collaboration with external partners. The breach might have implications for academic integrity as unauthorised access to academic records can compromise the credibility of student grades, academic achievements, and certifications. This may have radical consequences for both students and the university's reputation.

Data breach also have an impact on loss of trust and confidentiality. It compromises the confidentiality of sensitive information. Your personal information such as contact number, address, or identity card number might be used by criminals to make unauthorised purchases using the victim’s credit card or to apply for loans using the stolen information. Trade secrets, intellectual property, customer data, financial records, and other confidential information may be exposed, leading to a loss of competitive advantage, breach of contractual obligations, or damage to personal privacy.

Data Breach: Lesson Learned

In order to respond to this incident, individuals or organisations need to take immediate action to address the data breach and mitigate its impact. First of all, they can initiate an incident response team comprising IT professionals, legal experts, and communications specialists. Their primary task was to contain the breach, assess the extent of the compromise, and implement remedial actions to prevent further unauthorised access. The responsibilities of this team should include developing a proactive response plan, maintaining strong security best practices, and providing support for all incident handling measures. Aside from that, they should promptly communicate the data breach incident to affected individuals, emphasising transparency and offering guidance on safeguarding personal information.

Transparent communication is crucial in maintaining trust and ensuring that affected individuals are aware of the situation.

A comprehensive forensic investigation is mandatory to identify the breach's origins, the extent of compromised data, and the vulnerabilities that led to the breach. This investigation provides insights into the breach's cause and helps strengthen security measures to prevent future incidents. In Malaysia, collaboration can be done with relevant authorities, such as the Malaysian Communications and Multimedia Commission (MCMC) and the police, to investigate the breach, identify perpetrators, and ensure legal action is taken against those responsible. Collaboration with authorities is crucial to hold wrongdoers accountable and to deter future breaches.

On strengthening security measures, every organisation has to enhance their data security infrastructure by implementing robust access controls, encryption mechanisms, and intrusion detection systems. Regular security audits and vulnerability assessments were conducted to identify and rectify potential weaknesses in the IT systems. Audit trail is another method that can be applied to show who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and recovering lost transactions.

The recent data breach incident serves as a stark reminder of the importance of data security and privacy in an organization. While the incident has undoubtedly caused concerns and challenges, company’s effective response and comprehensive measures will demonstrate their commitment to addressing the breach's impact and reinforcing data protection practices. By continuously evaluating and strengthening security protocols, victims can rebuild trust, protect stakeholders' privacy and regain their customers' trust.

References

IBM. (2022). What is a data breach? https://www.ibm.com/topics/data-breach

Long Cheng, Fang Liu, Danfeng Yao. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. WIRES Data Mining and Knowledge Discovery, 5(3). https://doi.org/10.1002/widm.1211

Zareef Mohammed. (2021). Data breach recovery areas: an exploration of organization’s recovery strategies for surviving data breaches. Organizational Cybersecurity Journal: Practice, Process and People, Vol. 2 No. 1, 2022 pp. 41-59