pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

SINGAPORE'S DATA BREACH LANDSCAPE 2023/24

Data breaches have become a pressing global concern, with threat actors using ever-sophisticated tactics to exploit vulnerabilities and exfiltrating companies' and consumers data. This report provides an overview of the data breach landscape in Singapore **from January 2023 to December 2024**, focusing on key trends, observations and practical advice on how breaches can be mitigated.

KEY TRENDS

1 DATA BREACHES ON THE RISE

41% increase in large-scale[1] data breaches reported to the PDPC within a year.

2 CYBER INCIDENTS[2] THE LEADING CAUSE OF DATA BREACHES

Cyber incidents accounted for 82% of cases where the PDPC took enforcement action against companies that failed to protect their data because of weak security measures.

Ransomware accounted for **62%** of these cases.

3 MORE ORGANISATIONS FOUND IN BREACH OF THE PDPA

200% increase in PDPC enforcement actions[3], with organisations suffering financial consequences including:

Financial Penalties

Imposed by PDPC, which may be up to:
- 10% of annual turnover; or
- SGD 1 million, whichever is higher.

Remediation Costs

Costs incurred to contain, remediate and recover from data breaches.

Operational & Reputational Fallout

Loss of revenue from service outages, reputational damage and compensation payable to affected third parties.

[1] Data breaches affecting more than 500 individuals.

[2] Any event that involves unauthorised access to computer systems, networks or digital devices that may result in data exfiltration, such as through ransomware and phishing attacks.

[3] Refers to financial penalities, voluntary undertakings or directions issued by the PDPC against organisations that have failed to comply with the Personal Data Protection Act (PDPA).

B.E.S.T. MEASURES TO MITIGATE DATA BREACHES

B — **Back up** data regularly and securely offsite for restoration purposes.

E — **Encrypt** sensitive data (at rest and in transit) to protect them from hackers.

S — **Strengthen access controls** (e.g., strong passwords and multi-factor authentication) to reduce risk of unauthorised access.

T — **Track data assets and ensure timely maintenance of systems** with upgrades and patches to address vulnerabilities quickly.

CASE STUDY

Organisation X suffered a data breach impacting over 2 million user accounts when a malicious actor exploited a security vulnerability in its database. The breach was found to be a result of **inadequate security measures**, allowing the attacker to access and exfiltrate personal data, which was later found for sale on the Dark Web. The organisation was also fined by the PDPC for failing to implement reasonable security measures.

WHAT COULD BEEN DONE BETTER?

- **E** — **Encrypting** sensitive data stored within the affected database.
- **S** — **Strengthening** their access controls by protecting the affected database with perimeter controls (e.g., VPN, firewall).
- **T** — **Tracking** assets during data migration and ensuring that servers storing personal data are protected at all times.

As a best practice, the organisation should also implement adequate controls and processes outlined in the PDPC's **Guide on Data Protection Practices for ICT Systems.**

What should you do when a data breach occurs?

https://go.gov.sg/dbn-guide

Looking for the right solutions to fit your business needs?

https://go.gov.sg/dpo-ctoaas

To help us improve future reports, please share your feedback and suggestions with us at **https://go.gov.sg/dbreport-feedback**