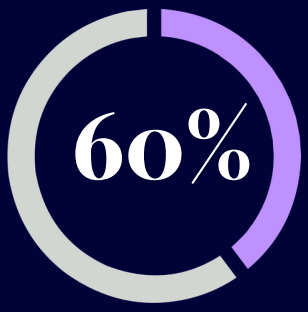
Data Breaches in Singapore: *Trends, Threats* & What To Do

This report provides an overview of the data breach landscape in Singapore in 2025, highlighting key trends and practical steps to strengthen data protection practices.



TREND 01

Cyber incidents remain a leading threat

Cyber incidents[1] continue to be the primary driver of large-scale[2] data breaches, accounting for 60% of cases where regulatory actions were taken.

Ransomware remains persistent, appearing across multiple sectors and organisation sizes.

RECOMMENDATION

Build simple, consistent habits

Not all breaches can be prevented but implementing B.E.S.T. can significantly reduce their likelihood and impact.

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 to reduce risk of unauthorised access

T — Track data assets and ensure timely maintenance of systems

TREND 02

Human error remains a persistent risk

Breaches caused by internal lapses have held steady over the past years, driven by two recurring contributors:

Admin errors — sending sensitive information to the wrong recipient, misconfiguring system access permissions, or skipping verification steps.

→ No significant change from previous year

System issues — incorrect system configurations, inadequate testing before deploying changes to live environments.

→ No significant change from previous year

RECOMMENDATION

Invest in Data Loss Prevention & Database-level Monitoring

Strong data loss prevention (DLP) controls and active monitoring help catch data mishandling before it escalates.

Monitor and set alerts for unusual activity
Flag unexpected spikes in data access, bulk exports, or unfamiliar logins — and respond immediately according to your data breach plan.

Block at the exit points
Automatically block large, suspicious, or unauthorised data transfers before they leave your systems.

[1] Any event that involves unauthorised access to computer systems, networks or digital devices that may result in data exfiltration (e.g., ransomware, phishing).
[2] Data breaches affecting more than 500 individuals.

↓ Continued on Page 2

OVERALL OBSERVATION

Data risks don't discriminate by size or sophistication

Breaches caused by cyber incidents and human oversight are consistent across industries, sectors, and organisation sizes.

MOST AFFECTED SECTORS

Case Studies & *What They Tell Us*

CASE STUDY 01

During a large-scale software migration exercise, Organisation A failed to ensure that security policies and related identifiers were properly carried over to the new system, leaving a gap that went undetected for months.

Threat actors then exploited the gap to access and exfiltrate customers' personal data, which was subsequently found offered for sale on the dark web.

This example illustrates the **consequences of a failure of process governance,** which could have been prevented by having a more rigorous system to flag out immediate risks.

CASE STUDY 02

Threat actors gained unauthorised access to Organisation B's servers on two separate occasions by exploiting vulnerabilities in a publicly accessible web application and dormant application that had not been decommissioned.

As a result, customers' personal data were exfiltrated and subsequently posted on web hacking forums.

The breach were primarily **due to system shortcomings, such as outdated web servers, absence of threat detection tools and multi-factor authentication**. Implementing these safeguards would have prevented the breach.

HOW TO MANAGE DATA BREACHES WHEN IT OCCURS

DATA PROTECTION ESSENTIALS FOR YOUR ORGANISATION

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