

WHEN SYSTEM MIGRATION GOES WRONG: LESSONS ON RESPONDING TO A DATA BREACH

MONTH :
October 2026

BY :
Sri Sarguna Raj, Steven
Cheok, Nicole Chong &
Syuhaini Safwan



WHEN SYSTEM MIGRATION GOES WRONG: LESSONS ON RESPONDING TO A DATA BREACH

Migrating IT systems is a routine undertaking. Organisations do so to modernise their infrastructure, reduce operational costs, or transition to cloud-based platforms. However, recent reported cyber incidents illustrate that system migration is not merely a technical exercise, it is also a compliance and governance event that warrants careful oversight.

During migration, apparently minor weaknesses such as overly permissive access settings, exposed credentials or inadequate segregation of legacy and new environments can create an entry point for unauthorised access. A technical incident can quickly become a data-protection, regulatory and reputational issue. In dealing with data breach incidents, how an organisation responds afterward matters more than the breach itself. A well-handled breach follows a clear sequence: containment, confirmation, timely reporting, and clear communication with those affected.

What that looks like in practice is set out below.

The First 24 Hours: Contain, Assess, Decide

Alongside containment, the incident response team, which should already exist on paper before a breach ever happens, should promptly assess whether the incident amounts to a personal data breach. Under the PDPA, this includes a breach, loss or misuse of personal

data, or unauthorised access to it. The question is not simply whether systems were compromised, but whether personal data was affected and whether the organisation has reason to believe that a personal data breach has occurred.

This assessment should be rapid, evidence-based and documented. An organisation does not need to wait until every forensic question is resolved before acting. At the same time, early containment measures, such as isolating affected systems, revoking credentials and preserving logs, should proceed immediately, even while the legal and technical assessment continues.

Know Your Clock: Reporting Obligations Are Not Negotiable

This is where the Personal Data Protection Act ("PDPA") lens matters. Under the PDPA 2024 amendments, notification to the Commissioner must be made as soon as practicable, and no later than 72 hours. For a network compromise, that 72-hour period begins running from the point the organisation confirms, through its own investigation, that the system has actually been breached, not from when the incident was first detected or suspected. A further 7 days is then given to notify affected individuals once the Commissioner has been notified. "We're still investigating" is therefore not a reason to delay confirming; the clock rewards organisations that investigate quickly, not ones that investigate slowly to buy time.

If the breach causes or is likely to cause significant harm to affected individuals, the data controller must also notify those individuals without unnecessary delay. The organisation should therefore assess harm in parallel with scope, including whether the compromised data could facilitate identity fraud, financial loss, unlawful misuse or other material adverse consequences.

Separate obligations may arise under the Cyber Security Act 2024 where an organisation has been designated as a National Critical Information Infrastructure (“NCII”) entity. In that case, the entity may need to notify National Cyber Security Agency (“NACSA”) and its relevant sector lead immediately upon becoming aware of a cyber-security incident or potential incident, provide prescribed initial particulars within 6 hours, and a full report within 14 days. The PDPA and NCII regimes can therefore operate in parallel, with different triggers, recipients and reporting timetables.

Building the Notification: What Regulators Expect to See

A notification submitted within the deadline, but lacking substance can create more problems than it solves. At minimum, a notification to the Commissioner should cover:

- The nature and scope of the breach.
- The categories and approximate number of individuals affected.
- The likely consequences of the breach; and
- The containment and remedial measures already taken or planned.

Where full details are not yet available, the PDPA framework allows for a phased notification, an initial report followed by supplementary updates as the investigation progresses. What is not acceptable is silence while facts are gathered.

Managing Stakeholders: Internal Alignment Before External Disclosure

A breach response fails almost as often on communication as it does on technical containment. Internally, there needs to be a single point of coordination, typically the Data Protection Officer (“DPO”) or a designated incident lead should coordinate the response and maintain a single, controlled information flow between IT, legal, senior management, the board and external advisers. Conflicting or premature statements from different parts of the organisation undermine both the regulatory response and public confidence.

Externally, affected individuals need to be told what happened, what data was involved, what the organisation is doing about it, and what steps they can take to protect themselves, in plain language rather than legal or technical jargon. Where the breach is likely to attract media or public attention, a holding statement prepared in advance, even before all facts are confirmed, prevents the organisation from being caught reacting rather than leading the narrative.

After the Notification: The Work Is Not Over

Regulatory notification is a milestone, not the finish line. Organisations should expect follow-up queries from the Commissioner or NACSA and should be prepared to demonstrate what remedial and preventive steps have been taken, not merely what happened. A well-contained breach with poor follow-up can still result in regulatory action, reputational damage, or both.

System migration can create cyber-security and data-protection risks, particularly where access controls, credentials, legacy environments or cloud configurations are not adequately managed. Many of these risks are foreseeable and preventable.

The more important lesson, however, is that when an incident does occur, the organisations that respond best are not necessarily those that never make a mistake. They are the ones that have already established a clear response plan, assigned decision-makers, tested escalation procedures and know how to act quickly when something goes wrong.

If your organisation does not yet have a data breach incident response plan or would benefit from review against the recent guidelines issued by the Personal Data Protection Commissioner ("PDPC"), feel free to reach out to our partners for a discussion.

This article was written by our Intellectual Property, Technology, Media, Sports,

Gaming & Data Protection partners, Sri Sarguna Raj, Steven Cheok Hou Cher, Nicole Chong & Syuhaini Safwan, with the assistance of Soo An Qi, Emily Ong Wenyen and Adriana Lee (Managing Associate, Associates & Pupil). It contains general information only. It does not constitute legal advice or an expression of legal opinion and should not be relied upon as such.