DPEX

DATA PROTECTION EXCELLENCE NETWORK

# RESEARCH ON ENFORCEMENT CASES IN SINGAPORE

*2016 - 2019*

STRAITS INTERACTIVE

# CONTENTS

## Introduction

Singapore Personal Data Protection Act was legislated in 2012 to protect the individual's personal data. It recognises both the rights of individuals, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes. It also provides for the establishment of a national Do Not Call (DNC) Registry.

## Objectives of report

To provide an analysis of the enforcement of the Singapore Personal Data Protection Act, in terms of:

- Overview of Annual trend
- Sectors
- Common breaches

## Methodology

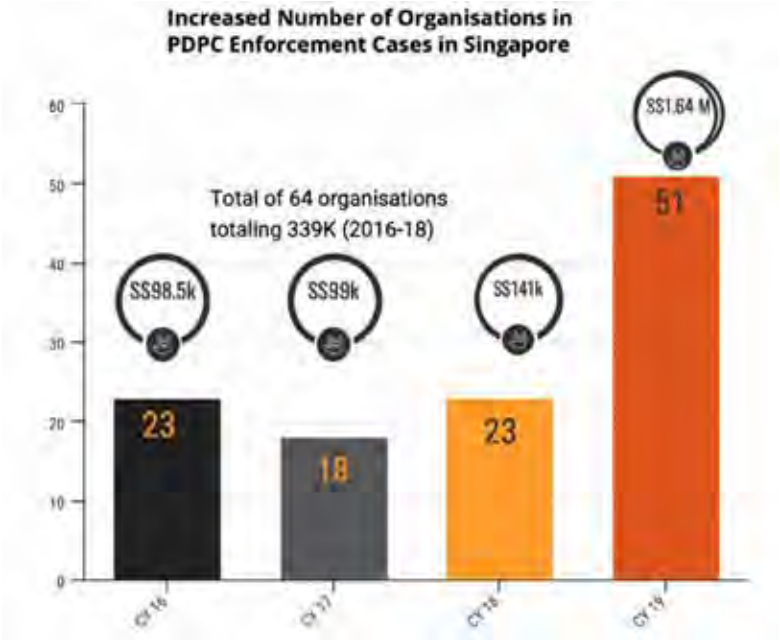
- Secondary Research by scanning and coding Singapore Personal Data Protection Commissioner's decision on the enforcement cases against the legislation
- Period: CY 2016-2019

https://www.pdpc.gov.sg/Commissions-Decisions/Data-Protection-Enforcement-Cases

https://www.pdpc.gov.sg/Legislation-and-Guidelines/Legislation

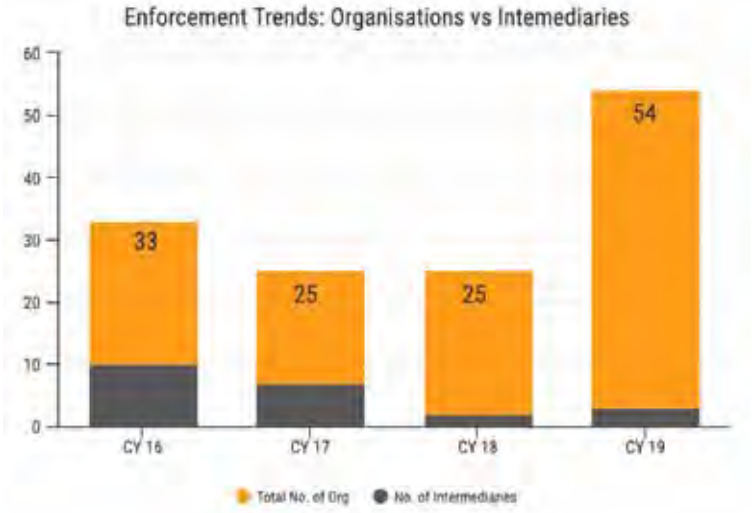
## Overview of Annual Trend

In the four years since the Act was legislated, the number of enforcement cases increased from 23 in CY'16 to 51 in CY'19.




2019 was a year when an anomaly occurred, the PDPC has imposed its highest financial penalties (to date), of $750,000 and $250,000 respectively on Integrated Health Information Systems (IHIS) and Singapore Health Services (SingHealth). The penalty was for "failure put in place adequate safeguards proportional to the harm that might be caused by disclosure of that personal data.", arising from a cyber attack on SingHealth's patient database system.

The number of data breaches were higher amongst organizations compared to data intermediaries.



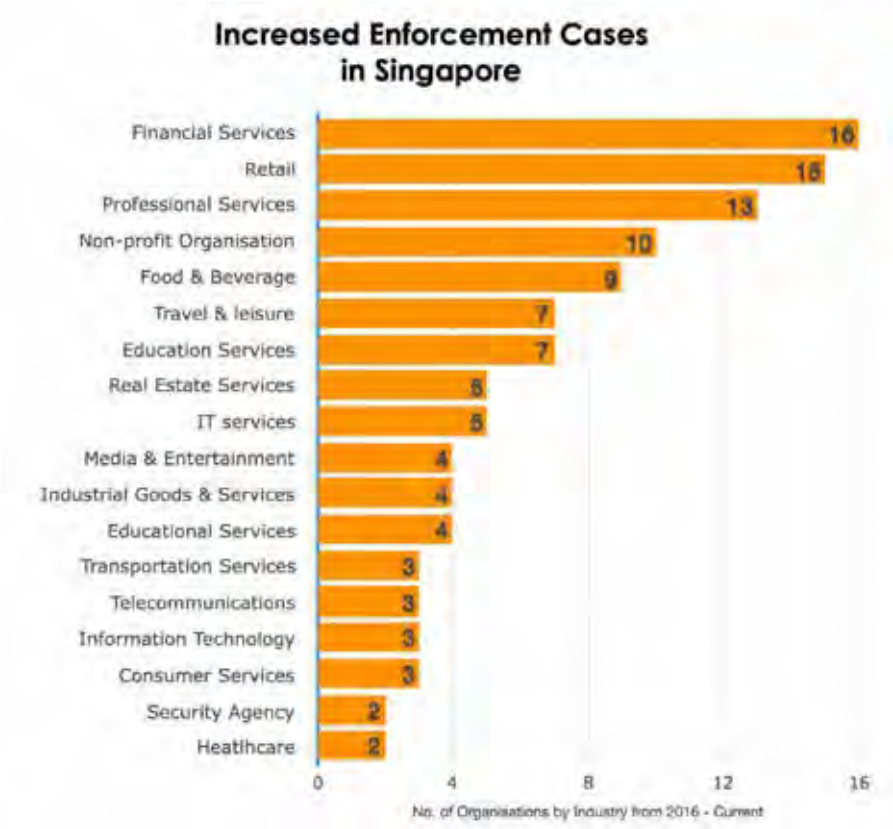
## By Sectors

No Industry is spared from enforcement, including non profit organisations. Generally the service sectors have been found to have a higher likelihood of breaches.

**Table 1- Enforcements by Industry**

| Vertical Industries | CY16 | CY17 | CY18 | CY19 | Total No. of Companies | % |
|---|---|---|---|---|---|---|
| Consumer Services | | | | 3 | 3 | 3% |
| Education Services | 1 | 1 | 3 | 2 | 7 | 6% |
| Educational Services | | 1 | | 3 | 4 | 3% |
| Financial Services | 2 | 4 | 4 | 6 | 16 | 14% |
| Food & Beverage | 4 | 1 | 1 | 3 | 9 | 8% |
| Heatlhcare | | | | 2 | 2 | 2% |
| Industrial Goods & Services | | 2 | 2 | | 4 | 3% |
| Information Technology | | | | 3 | 3 | 3% |
| IT services | 3 | | | 2 | 5 | 4% |
| Media & Entertainment | 2 | | 1 | 1 | 4 | 3% |
| Non-profit Organisation | 3 | 1 | 5 | 1 | 10 | 9% |
| Professional Services | | 1 | 1 | 11 | 13 | 11% |
| Real Estate Services | 1 | 2 | 1 | 1 | 5 | 4% |
| Retail | 5 | 2 | 2 | 6 | 15 | 13% |
| Security Agency | 1 | 1 | | | 2 | 2% |
| Telecommunications | | 1 | | 2 | 3 | 3% |
| Transportation Services | | | 1 | 2 | 3 | 3% |
| Travel & leisure | 1 | 1 | 2 | 3 | 7 | 6% |
| **Total No. Of Companies** | **23** | **18** | **23** | **51** | **115** | **100%** |

Generally the financial and consumer lifestyle service sectors have been found to suffer a higher likelihood of data breach. The financial and consumer lifestyle service sectors tend to face higher risk of breach and enforcements.



## Common Breaches

The most frequent cause for enforcement is the failure to adequately protect personal data due to security lapse.

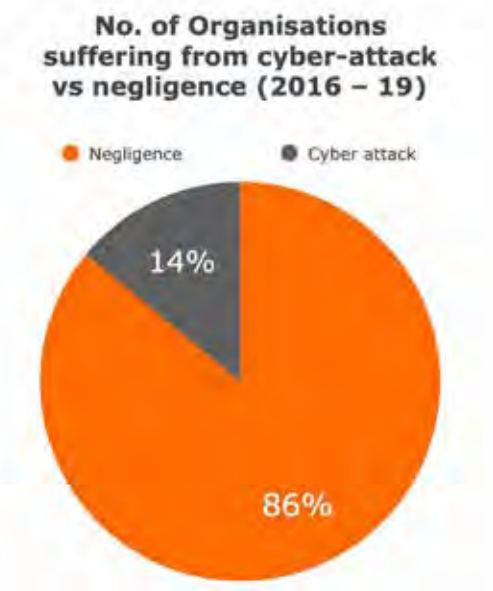
Table 2- Causes of Breach

| | CY16 | CY17 | CY18 | CY15 | Grand Total | % |
|---|---|---|---|---|---|---|
| 11 (Compliance/DPO) | 3 | 1 | 1 | 7 | 12 | 10% |
| 12(a) Policies | 3 | 1 | 5 | 15 | 24 | 21% |
| 13 Consent | 5 | 2 | 5 | 4 | 16 | 14% |
| 18 Purpose Limitation | 2 | | 4 | 1 | 7 | 6% |
| 20 Notification | 4 | 1 | | 3 | 8 | 7% |
| 21 Access | | | | | | 0% |
| 23 Accuracy | | | | | | 0% |
| 24 Protection | 18 | 16 | 17 | 41 | 92 | 80% |
| 25 Retention | | 1 | | 1 | 2 | 2% |
| 26 Transfer | | | | 2 | 2 | 2% |
| **# Organisation** | **23** | **18** | **23** | **51** | **115** | |

*Note: There could be multiple breaches in a single organisation*

Of the 92 cases in failure to protect, the large portion is due to negligence rather than a deliberate cyber attack.

Only 14% of those who breached the protection obligation were linked to an actual cyber attack/hacking.



The trend that cyber attack/hacking forms only a small fraction of breach in data protection has been consistent since the enforcement commenced in 2016 as illustrated in Table 3.

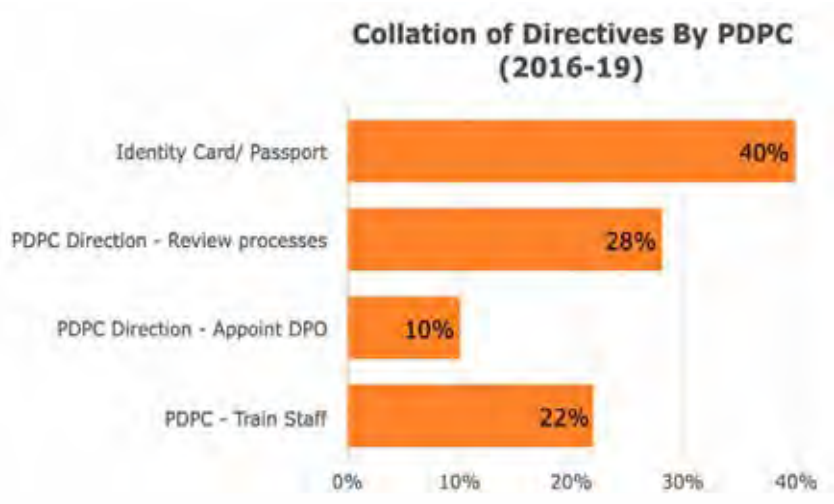
**Table 3- Causes of Breach**

| Protection Obligation | CY16 | CY17 | CY18 | CY19 | Grand Total |
|---|---|---|---|---|---|
| Cyber Attack/Hacked | 8 | 1 | 0 | 6 | 15 |
| Negligence | 10 | 15 | 17 | 48 | 90 |
| **Grand Total** | **18** | **16** | **17** | **54** | **105** |
| **%** | 44% | 6% | 0% | 11% | 14% |

Further details were identified in the failure to protect personal data and in collation of case reports, the top 10 causes are:

1. Untrained staff
2. No data protection policies
3. Inadequate security controls
4. Lack of appropriate SOPs
5. Weak passwords
6. Poor system/software design
7. Sending to wrong recipients
8. Failure to verify the accuracy of processed data
9. System security not audited regularly
10. Error in processing/printing

To help remediate the situation, the PDPC provides directions and it can be seen that the lack of training that underlies the common breaches faced by the organisations.

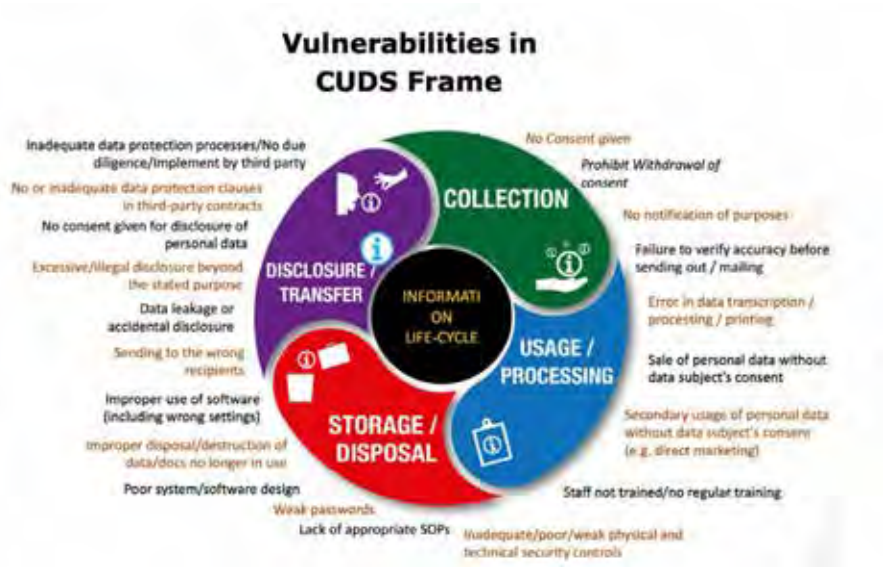


This can be seen to be the trend in the four years since PDPA enforcement began: appointing an qualified DPO, training of staff and the know-how to review operation in compliance with data protection relates to the education and training of staff in data protection.

**Table 4-Directives issued by PDPC**

| | CY16 | CY17 | CY18 | CY19 | TOTAL |
|---|---|---|---|---|---|
| Identity Card/ Passport | 9 | 6 | 15 | 16 | 46 |
| PDPC Direction - Review processes | 8 | 7 | 3 | 14 | 32 |
| PDPC Direction - Appoint DPO | 4 | 1 | 1 | 6 | 12 |
| PDPC Direction - Train Staff | 3 | 6 | 3 | 13 | 25 |
| **Total No. Of Organisations** | **18** | **23** | **51** | **115** | |

Integrating the common causes behind infringement and resulting enforcement in PDPA, it can be seen they are common in the various points of collection, processing (usage), storage and disclosure of personal data.



## Discussion & Conclusion

- Number of data incidents and enforcement has been increasing.
- Data Incidents and enforcement occurred across all industry sectors especially the financial and lifestyle sectors.
- 80% of all cases are due to breach of protection obligation
- Most cases due to negligence which of which failure in operational compliance formed the major portion.
- Many had Breakdown of/no standard operating procedures
- Most breaches can be avoided. The following are some common vulnerabilities:
  - Lack of awareness/ underestimated risks
  - Identified risk – but no actions to address them
  - Identified risk, planned the actions – but no implementation
  - Identified risks, actions were implemented – but NOT effective
- Risk can be minimized and incidents mitigated with proper processes and skill set.

## About Straits Interactive

Straits Interactive delivers end-to-end governance, risk and compliance solutions that enable trusted business and responsible marketing, especially in the area of data privacy and protection. Recently Data Protection Trustmark (DPTM) certified, we help businesses achieve operational compliance and manage risks through a combination of cloud technology and professional services. Our quest for innovation has led to us being recognised and awarded Intercon's Top 50 Tech Companies (in recognition of the company's contribution to technology) and APAC Business Headlines' Company of the Year, 2019. Our software-as-a-service solutions include DPOinBOX and Governance, Risk & Compliance System (GRACIAs), all of which are supported by professional services that include advisory services, audits, and training. More information about the company can be found on www.straitsinteractive.com.

## About the Data Protection Excellence (DPEX) Network

The Data Protection Excellence (DPEX) Network is the first of its kind facility in the ASEAN region whose aim is to provide leadership, best practices, training, research and support for all things surround data privacy from an operational perspective. This collaboration of partnerships comprise accreditation bodies, law firms, universities and organisations who provide professional services and technologies relating to data privacy. An ever-growing network, members currently include Straits Interactive, Singapore Management University, International Islamic University of Malaysia, De LaSelle University, Philippines, IAPP, EXIN, OCEG and Lexxion amongst others. More information about DPEX Network can be found at www.dpexnetwork.org

**For media enquiries, please contact:**
Ms Angela Schooling
Marketing and Communications Director
Mobile: (65) 98222625