Centre for Technology, Robotics, Artificial Intelligence & the Law
Faculty of Law

NUS Law Working Paper 2021/021

NUS Centre for Technology, Robotics, Artificial Intelligence & the Law Working Paper 21/03

Cybersecurity and Data Protection: Some Empirical Observations, and A Lacuna in the PDPA?

Shaun Lim

Research Assistant, Centre for Technology, Robotics, Artificial Intelligence & the Law, Faculty of Law, NUS

[October 2021]

Note: The views expressed in each paper are those of the author or authors of the paper. They do not necessarily represent or reflect the views of the National University of Singapore.

CYBERSECURITY AND DATA PROTECTION: SOME EMPIRICAL OBSERVATIONS, AND A LACUNA IN THE PDPA?

On the occasion of amendments to the Personal Data Protection Act (PDPA), it is timely to review past decisions by the Personal Data Protection Commission (PDPC) to determine what a reasonable standard of data protection in relation to cybersecurity is. In general, a review of PDPC cases confirms that cybersecurity is rising in prominence as an aspect of data protection, and that cybersecurity-related data breaches tend to be more severe in impact in terms of the amount of personal data breached. To stave off data breaches, data organisations would do well to adopt a defence in depth strategy, and to ensure that their data intermediaries and vendors are well-apprised of their data protection obligations; however, it appears that non-data intermediary vendors can cause data breaches for which no liability can attach. While this may not be a desirable state of affairs, it is also not easy to remedy within the current data protection paradigm of the PDPA.

Shaun **LIM**
LLB (Hons) (National University of Singapore);
Advocate and Solicitor (Singapore);
Research Assistant, Centre for Technology, Robotics, Artificial Intelligence & the Law, Faculty of Law, National University of Singapore

Introduction

Since the coming into force of the Personal Data Protection Act[1] ("PDPA") in 2014, the Personal Data Protection Commission of Singapore ("PDPC") has published grounds of decision for its enforcement actions beginning in 2016, as well as a smaller number of case summaries besides (collectively "the PDPC decisions").

Anecdotal observation of these PDPC decisions suggest two broad trends. First, cybersecurity-related data breaches are increasing in frequency.[2] Broadly speaking, this is to be expected given the accelerating pace of technological adoption in today's digitalised economy, as well as a rise in general cybercrime such as phishing, malware, and ransomware attacks.[3] Second, very few investigations conducted by the PDPC have resulted in findings that all the data organisations concerned have adequately discharged their data protection obligations.[4] Collectively, these seem to suggest that a cybersecurity-related data breach will generally – but not always[5] – result in a finding of breach of the Protection Obligation.

This paper therefore aims to answer two research questions. First, based on PDPC decisions, it aims to quantify the difference in impact that lax cybersecurity measures (i.e. in cases where the PDPC have made findings of breach) have upon personal data protection, not least in terms of the amount of data exposed and the modalities of exposure. Second, it aims to identify the legal standard of what

[1] *Personal Data Protection Act 2012* (No 26 of 2012, Sing)
[2] See Cyber Security Agency of Singapore, *Singapore Cyber Landscape 2020*, pp 13, 19.
[3] *Ibid* at pp6-7.
[4] See *infra* text accompanying note X
[5] *Re BHG (Singapore) Pte Ltd* [2017] SGPDPC 16 at [1].

constitutes a reasonable level of cybersecurity measures that data organisations can take to discharge their data protection obligations.

This is all the more significant given that Singapore is shifting – or has shifted – its general cybersecurity strategy towards an "assume breach" mindset rather than a "prevent breach" mindset.[6] It is entirely possible that if, moving forward, the PDPC considers an "assume breach" mindset to be the default cybersecurity threat assessment that a data organisation should take, this could change the standard of reasonableness of cybersecurity measures that data organisations are expected to undertake. It is therefore timely to examine the entire body of PDPC decisions to determine what reasonable cybersecurity measures currently look like.

PDPC Decisions

A total of 184 PDPC decisions were collated from the Commission's Decisions section of the PDPC's website,[7] split into 140 grounds of decisions and 44 case summaries, and with a cutoff date of 12 August 2021.[8] The 140 grounds of decisions are straightforward as a record, as they represent a complete record of the investigations that have resulted in formal enforcement decisions being issued since 2016, and have been reprinted as such in the annual Personal Data Protection Digest ("PDP Digest"), the official publication of the PDPC.

However, the status of case summaries is a lot less straightforward. The 44 case summaries collected from the PDPC's website date only from 2019, representing a change in PDPC's policy as to case summaries. Between 2016 and 2019, a few case summaries were published only in the PDP Digest.[9] All of these pre-2019 case summaries resulted in findings that the organisation in question was not in breach, or even if in breach, was at most issued an advisory notice.[10]

From 2019 onwards, however, the PDPC has begun the practice of releasing case summaries independently on its website, alongside the grounds of decisions.[11] More notably, these case summaries now encompass more types of formal enforcement action taken against data organisations such as warnings, directions, and financial penalties.

It could be said that case summaries released from 2019 are to the grounds of decisions what unreported decisions are to reported decisions – demonstrations of the carrying out of enforcement

[6] Ministry of Communications and Information, "Minister for Communications and Information Josephine Teo in Tallinn, Estonia, to share experiences and forge partnerships for a thriving and secure digital future" <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2021/9/minister-for-communications-and-information-josephine-teo-in-tallinn-estonia-to-share-experiences-and-forge-partnerships-for-a-thriving-and-secure-digital-future?page=6> (accessed 21 September 2021)

[7] PDPC, *Commission's Decisions* <https://www.pdpc.gov.sg/Commissions-Decisions> (last accessed 21 September 2021)

[8] This was the publication date of the last summary within the dataset, *Re Singapore Telecommunications Limited* (12 August 2021), DP-2007-B6607.

[9] 19 case summaries were printed in the 2017 PDP Digest, 4 case summaries in the 2018 PDP Digest, and 1 case summary in the 2019 PDP Digest. There is a one-year offset as grounds of decision and case summaries are generally published in the PDP Digest of the subsequent year, so the 19 case summaries published in the 2017 PDP Digest are actually from investigations that concluded in 2016.

[10] All of the 5 case summaries from the 2018 and 2019 PDP Digests resulted in a finding of no breach. Of the 19 in the 2017 PDP Digest, 5 advisory notices were issued to remind organisations to comply with their obligations under the PPDA (including 2 for review applications then brought under s28(1) of the PDPA, now s48H(1) of the PDPA), with outright findings of no breach in the remaining 14.

[11] These case summaries are still published in the PDP Digest – indeed, the case summaries from 2019 that were on the PDPC's website (*supra* note 7) appear in the 2020 PDP Digest.

action by the PDPC in cases which are straightforward and re-tread trite law, with grounds of decisions reserved for cases which necessitate a fuller examination of the ambit of the relevant data protection obligations. For that reason, the case summaries released from 2019 are assembled for this study as valuable data points in their own right, but are sufficiently distinct from the full grounds of decisions that it appears prudent to the author to process them separately as their own distinct subset of cases.

Data coding

After the collation of the PDPC decisions, each PDPC decision was read closely to extract information relevant for analysis. Because multiple parties may be named as subjects of a PDPC decision,[12] and the PDPC can make independent findings of breach or no breach against each subject of a PDPC decision,[13] data coding must distinguish between case-level and party-level attributes. In addition, as previously mentioned, case summaries were coded separately from the grounds of decision because of their drastically simplified structure.

This resulted in the creation of three tables, which were further broken down into subtables for convenience in data handling as follows:

1. Cases
    a. Key
    b. Facts
2. Parties
    a. Sections
3. Summaries

Key (Case level)

This subtable indexes every ground of decision issued by the PDPC to form the basis of all other tables via cross-referencing (except the Summaries table, which is independent), and also captures citation information and the case number issued to it by the PDPC.

Facts (Case level)

This subtable captures the following notable attributes of each grounds of decision, as follows:

Complaint source

This field captures whether the grounds of decision arose from a complaint by an individual member of the public, voluntary notification to the PDPC by the allegedly breaching data organisation, both, or by other means, such as the PDPC being notified by other government agencies[14] or acting on a tip-off.[15]

Brief description

This field classifies each case into one of the eight following categories:

- Accidental disclosure via attachments (7 cases)
- Deliberate hacks (21 cases)
- Personal data disclosed in the course of a dispute (7 cases)
- Lack of data protection policies (4 cases)

[12] See e.g. *Re K Box Entertainment Group Pte Ltd and anor* [2016] SGPDPC 1, *Re Jiwon Hair Salon Pte Ltd and ors* [2018] SGPDPC 2.

[13] See e.g. *Re Central Depository (Pte) Limited and anor* [2016] SGPDPC 11, *Re Times Software Pte Ltd and ors* [2020] SGPDPC 18t

[14] See e.g. *Re Ncode Consultant Pte Ltd* [2019] SGPDPC 11 at [2]

[15] See e.g. *Re Club the Chambers* [2018] SGPDPC 24 at [4]

- Non-mail physical disclosure of personal data (15 cases)
- Mailing errors, whether via physical letters or email (18 cases)
- Online exposure of personal data (52 cases)
- Others (20 cases)

This categorisation is somewhat rough and ready, and describes the circumstances leading to the discovery of the primary breach of data protection obligations in each case. While the PDPC occasionally discovers secondary breaches of data protection obligations on further investigation,[16] as the discovery of those secondary breaches is contingent on an investigation being initiated for the discovery of the primary breach in the first place, the decision was made to restrict categorisation to the circumstances of the primary breach.

It is arguable that there is a grey area between the online exposure of personal data and a deliberate hack. For instance, in cases involving URL manipulation,[17] it is arguable that changing the URL is itself a hack. Hacking tends to connote an aspect of illegal, non-permitted, or unauthorised access to the computer that has been hacked.[18] The persons in these cases who discovered the URL manipulation vulnerability often discovered the vulnerability by amending a URL which they might have been legitimately given in the course of their dealings with the data organisation. In that sense, by manipulating the URL and accessing the personal data of other persons, their actions were unauthorised and therefore arguably a "hack".

For the purposes of this paper, however, the term "hack" denotes cases where there was clear malign intent, such as the deletion or encryption of a database,[19] or clear evidence of an advanced persistent threat.[20] All other cases where the exposure (and discovery thereof) of personal data online occurred due to happenstance or inadvertence will be classified more generically as the online exposure of personal data.

Whether or not the case had cybersecurity aspects

This field captures whether or not each case bears any cybersecurity aspects.

Defining Cybersecurity

Before the PDPC decisions can be parsed for relevance to cybersecurity, we first need a working definition of cybersecurity. The PDPA itself does not contain a specific definition of cybersecurity, being concerned in general with personal data regardless of the form in which it is held. Therefore, we have to look elsewhere for a suitable legal definition, which we can find in s2 of the Cybersecurity Act 2018 ("CSA")[21] as follows:[22]

[16] See e.g. *Re Universal Travel Corporation Pte Ltd* [2016] SGPDPC 4 and *Re Singapore Taekwondo Federation* [2018] SGPDPC 17 where the PDPC found, during the course of investigations, that the data organisations were also liable for breaches of data protection obligations other than the Protection Obligation, and were dealt with accordingly.

[17] See e.g. *Re InfoCorp Technologies Pte Ltd* [2019] SGPDPC 17, *Re Fu Kwee Kitchen Catering Services and anor* [2016] SGPDPC 14

[18] See e.g. "hack", *Merriam-Webster*, <https://www.merriam-webster.com/dictionary/hack> (accessed 21 September 2021), and "hack", *Cambridge Dictionary* <https://dictionary.cambridge.org/dictionary/english/hack> (accessed 21 September 2021)

[19] See e.g. *Re DS Human Resource Pte Ltd* [2019] SGPDPC 16, *Re Ncode Consultant Pte Ltd* [2019] SGPDPC 11

[20] See *Re Singapore Health Services Pte Ltd and anor* [2019] SGPDPC 3

[21] *Cybersecurity Act 2018* (No 9 of 2018, Sing), s2

[22] See also general definitions of cybersecurity (Merriam-Webster, Cybersecurity https://www.merriam-webster.com/dictionary/cybersecurity) and definitions by other governmental agencies (Cybersecurity and

> "cybersecurity" means the state in which a computer or computer system is protected from unauthorised access or attack, and because of that state –
>
> (a) the computer or computer system continues to be available and operational;
> (b) the integrity of the computer or computer system is maintained; and
> (c) the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained[.]

Within the context of protecting personal data contained in digital media (hereinafter "digitalised personal data"), such as computers and computer systems,[23] this definition of cybersecurity has many overlaps with the Protection Obligation, one of the nine data protection obligations under the PDPA,[24] which reads in full as follows:

> An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent –
>
> (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and
> (b) the loss of any storage medium or device on which personal data is stored.

In the PDPA, "unauthorised access, collection, use, disclosure, copying" overlaps with the CSA criterion of "information confidentiality", since keeping information confidential must necessarily encompass the prevention of unauthorised access, collection, use, disclosure, and copying of that information. Likewise, "modification or disposal" can be equated with the CSA criterion of "information integrity", since data that has been modified or destroyed can no longer be said to maintain its integrity. In addition, "making reasonable security arrangements" under the PDPA, as applied to computers and computer systems, imply the creation of a "state in which a computer or computer system is protected from unauthorised access or attack" under the CSA. Since the standard in the PDPA is one of reasonableness, this state of protection is not necessarily absolute,[25] but the making of any reasonable security arrangement in relation to a computer or computer system must necessarily result in creating a state of some protection against at least some types or degrees of unauthorised access or attack on that computer or computer system.

Furthermore, the ambit of the PDPA in governing the "collection, use and disclosure"[26] of personal data also overlaps with the phrase "stored in, processed by or transmitted through" in the definition of cybersecurity in the CSA, at least when applied to digitalised personal data. The collection of digital personal data must imply the recording of that data on some medium somewhere and hence its storage for the purposes of the CSA. The use of digitalised personal data must imply some degree of processing by a computer or computer system, however rudimentary it may be, in order to render that personal data into a human-comprehensible form. And lastly, for a data organisation to disclose

Infrastructure Security Agency, Security Tip (ST04-001): What is Cybersecurity (Nov 14 2019) <https://us-cert.cisa.gov/ncas/tips/ST04-001> (accessed 21 September 2021)

[23] *Supra* note 21

[24] *Supra* note 1 at s24.

[25] *Supra* note 5

[26] See e.g. *supra* note 1 at s3.

digitalised personal data to an entity outside the data organisation, that must also imply the use of a computer to transmit said personal data.[27]

These overlaps make clear that at least in relation to digitalised personal data, taking reasonable security arrangements to protect that personal data must imply securing that personal data against unauthorised access or attack, and hence involve some aspects of cybersecurity. Therefore, carrying out the Protection Obligation in respect of digitalised personal data is tantamount to ensuring the cybersecurity of that digitalised personal data. However, cybersecurity and the Protection Obligation do not perfectly overlap, and there are cases where the Protection Obligation is breached without cybersecurity being involved.

For instance, a common breach archetype is the accidental transmission of digital personal data via email.[28] This technically results in unauthorised access to personal data, and hence *prima facie* also results in a breach in the confidentiality of information transmitted through a computer or computer system. However, there is a distinction in that the unauthorised access is foisted on the unintended recipients by the breaching data organisation, as opposed to an unauthorised person forcibly gaining access in some way to that personal data without the active connivance of the breaching data organisation.[29] It is therefore arguable that despite the technical breaking of limb (c) of the definition of cybersecurity above (and hence a breach in the cybersecurity of the relevant computer system as a whole)[30], this breach is a matter of human error which does not fundamentally impugn the cybersecurity of the computer or computer system. Furthermore, the accidental transmission of digitalised personal data alone, without more, does nothing to change the cybersecurity posture of the computer or computer system in question. It is a different matter if the human error resulted in a change in the cybersecurity posture of the computer or computer system,[31] or caused a failure to implement any cybersecurity measures at all in the first place.

The PDPC's publication of separate guides on these topics supports this distinction, as this suggests that in data protection practice, cybersecurity and accidental disclosure are indeed considered separate by the sectoral regulator no less. The Guide to Printing Processes for Organisations (with a section on the generation of emails) and the Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data deal with preventing accidental disclosure of personal data, while the Guide to Building Websites for SMEs, Guide to Securing Personal Data in Electronic Medium [sic] and, to a lesser extent, the Guide to Data Protection by Design for ICT systems deal with cybersecurity concerns like passwords, firewalls, and online vulnerabilities.

From the foregoing, the following approach will be taken in classifying PDPC decisions as involving cybersecurity for the purposes of this paper. First, only cases where a data organisation's Protection Obligation is in question, regardless of any eventual finding of breach or no breach, will be considered

[27] Under the CSA, a computer includes a data processing device performing storage functions, so even the handing over of digital personal data via a physical storage medium like a hard drive will still be considered the transmission of data through the use of a computer.

[28] See e.g. *Re Habitat for Humanity Singapore Ltd* [2018] SGPDPC 9 at [5], *Re SAFRA National Service Association* [2019] SGPDPC 45 at [4].

[29] As opposed to "passive" connivance by having lax or non-existent cybersecurity measures.

[30] The three limbs of the definition of cybersecurity are conjunctive, meaning that a breach of any one of these is a breach of the cybersecurity of the relevant computer or computer system.

[31] Such as falling victim to a phishing attack utilising social engineering (although this is not the outward transmission of digitalised personal data *per se*): see *Re ST Logistics Pte Ltd* [2020] SGPDPC 19 at [4]. Even so, employees falling for a phishing attack need not necessarily result in a finding of breach: see generally *Re Singapore Telecommunications Limited* (12 August 2021), DP-2007-B6607.

capable of bearing any cybersecurity aspects for the purposes of this paper. In other words, if a data organisation is under investigation for breaches of data protection obligations other than the Protection Obligation, there is no occasion to examine the cybersecurity practices of the data organisation. Second, a PDPC decision will be treated as involving cybersecurity only if it involves digitalised personal data as well as unauthorised access to or attack on said digitalised personal data, as cybersecurity elements are not necessarily invoked every time a data organisation's discharge of its Protection Obligation is in question. In sum, cybersecurity-related PDPC decisions will be a subset only of PDPC decisions where the Protection Obligation is in question.

This granular classification allows us to quantify the exact proportion of PDPC cases which involve cybersecurity, as well as the impact of these cases in terms of the data breaches involved. A case will be considered as being capable of bearing any cybersecurity aspects only if a breach of the Protection Obligation is involved, otherwise it will be coded as "NA" (not applicable). The facts of each case involving a breach of the Protection Obligation are then read to determine if cybersecurity aspects are involved.

Volume of affected personal data

This field records the amount of personal data, in terms of unique individuals, that were affected by the breach under investigation in each grounds of decision. In general, the PDPC appears to pay attention to two different types of affected personal data: personal data that was actually exposed in a data breach (hereinafter "breached personal data") and personal data that was rendered vulnerable in the breach, but for which there was no direct evidence of exposure or exfiltration (hereinafter "vulnerable personal data").

As with the classification of cases into deliberate hacks versus online exposure, there is yet another grey area between breached personal data and vulnerable personal data, as the nature of the breach itself affects whether the personal data is considered breached or vulnerable. For instance, in *Re Singapore Health Services Pte Ltd and anor*,[32] servers hosting electronic patient health records were hacked, with 1.5 million records actually exfiltrated, and a total of more than 5 million rendered vulnerable.[33] Therefore, the 1.5 million records were considered as breached personal data, with the 5 million considered vulnerable personal data. However, in other cases, data that was merely exposed, without any indications of exfiltration, or even any proof that the data was actually accessed, was counted as the breached personal data instead.[34]

This inconsistency is understandable given the myriad ways in which personal data can be exposed. For instance, personal data breached because of a deliberate hack is generally disclosed only to the hackers if at all,[35] rather than made available over the Internet for all and sundry to see when a configuration error is to blame.[36] In the former case, server logs can capture personal data that was actually affected or exfiltrated,[37] whereas in the latter case, it is sometimes impossible to determine whether the exposed personal data was exfiltrated or even seen, if server and access logs are lacking.

[32] [2019] SGPDPC 3

[33] *Ibid* at [139].

[34] See e.g. *Re The Travel Corporation (2011) Pte Ltd* [2019] SGPDPC 42, where a hard disk containing over 16 thousand personal data sets was lost, with no findings made as to the ultimate fate of the hard disk – and therefore whether the data was entirely lost or whether it was recovered and/or accessed by some as-yet unknown third party.

[35] See e.g. *Re Singapore Health Services Pte Ltd and anor* [2019] SGPDPC 3. See also *Re DS Human Resource Pte Ltd* [2019] SGPDPC 16, where the hacked data was simply deleted from the data organisation's servers.

[36] See e.g. *Re Dimsum Property Pte Ltd* [2018] SGPDPC 20, *Re National University of Singapore* [2017] SGPDPC 5

[37] See e.g. *Re Singapore Health Services Pte Ltd and anor* [2019] SGPDPC 3 at [32].

Due to these differences in breach modalities, one breach's vulnerable personal data can be another breach's breached personal data. However, this also makes the volume of personal data involved in the breach an imperfect proxy for the impact of the data breach. At this time, absent any further analyses into breach modalities, analyses based on the volume of personal data involved in data breaches must bear this inconsistency in mind without necessarily having a way to correct for it. Nevertheless, the order of magnitude of exposed personal data still serves as a relative indicator of the severity of the data breach.

Sections (Party level)

This table records each entity that was a subject of investigation by the PDPC, and further records the sections that they were investigated under. It informs the classification of cases as bearing cybersecurity aspects, as well as some of the other analyses throughout this paper.

Summaries

This table records the 40 case summaries that were released by the PDPC from 2019 onwards. Of the 40 cases, 27 related to cybersecurity, out of 37 cases that involved the Protection Obligation. The volume of personal data rendered vulnerable[38] ranged from 522,722[39] to 3,[40] for a mean of 19,298 personal data sets rendered vulnerable, and a median of 112 personal data sets rendered vulnerable overall. These figures are not too far off from the mean of 21,159 personal data sets breached and the median of 128 personal data sets breached in the main grounds of decisions dataset, which suggests that the distinction between cases published as case summaries and cases published as full grounds of decisions does not lie in the facts of the case.

Overall Analysis

General trends

The number of cases involving cybersecurity seems to have come to a head in 2020. The explanation for this phenomenon, however, would appear not to reside with the rise in electronic transactions and electronic operations that accompanied the COVID-19 pandemic, as the majority of the grounds of decision published in 2020 were initiated in 2019 or earlier.

Each decision contains a PDPC-assigned case number, which can be used to reverse engineer the approximate date on which the PDPC initiated the investigation ("investigation initiation date"), as the case number apparently comes in the following standard format:

> DP-YYMM-[4/5-digit alphanumeric code][41]

This is corroborated by several grounds of decisions, where the PDPC notes in the statement of facts that it received complaints, voluntary notifications, or began investigations in the same month/year combination as reflected in the case number.[42]

[38] The case summaries do not distinguish between volume of personal data breached and volume of personal data rendered vulnerable to breach.

[39] *Re Webcada Pte Ltd* (10 June 2021), DP-2009-B6931

[40] *Re Horizon Fast Ferry Pte Ltd* (16 October 2020), DP-1912-B5465

[41] Each 4/5-digit alphanumeric code to date consists of the letter A or B, followed by a numeric code that is either 3 or 4 digits long. The import of the letter is not endogenously apparent on a cursory examination of the entire dataset: there is for instance no correlation with whether the case arose from a complaint or a voluntary notification.

[42] See e.g. *Re Horizon Fast Ferry Pte Ltd* [2019] SGPDPC 27 at [1] and *Re Friends Provident International Limited* [2019] SGPDPC 29 at [1]. However, cf *Re Marshall Cavendish Education Pte Ltd* [2019] SGPDPC 34 where the

If the derivation of the investigation initiation date is reasonably reliable, then it is possible to use the investigation initiation date and the date of the grounds of decision itself to approximate the time , in months, taken by the PDPC to complete its investigations. This indicates that, over the 144 grounds of decision, the PDPC takes approximately 15 months to complete its investigations, with a median of 13.5 months, a mode of 10 months, a maximum investigation time of 34 months[43] and a minimum investigation time of three months.[44]

This means that, even before the COVID-19 pandemic ushered in a paradigm shift in the ways organisations operated, data breaches involving cybersecurity were already on the rise. Neither is the answer the apparent rise in ransomware: research by cybersecurity providers shows that prior to the COVID-19 pandemic, ransomware attacks were declining in frequency,[45] or at best holding steady compared to the past two years.[46] This is corroborated by looking at the circumstances of the cases involving cybersecurity. While there have always been a certain amount of data breaches caused by deliberate hacks, including ransomware attacks, in all years other than 2016 and 2021,[47] the exposure of data online has always been a far more significant contributor to data breaches involving cybersecurity than data breaches caused by deliberate hacks.

At this point, it is therefore unclear exactly why cases with cybersecurity aspects form such a large proportion of cases in 2020. The difficulty in determining the apparently anomalous trends in 2020 may stem in part from the difficulty in correlating the publication of PDPC decisions to data protection trends in wider industry practice. On top of the inherent time delay caused by investigations, not every complaint to the PDPC results in an investigation,[48] and there are investigations that do not originate from complaints.[49] The PDPC itself also acknowledges in its Guide to Active Enforcement that not every complaint can result in an investigation, much less an enforcement decision:[50]

case number would indicate an investigation begun in April 2017, but the PDPC notes that the data organisation first became aware of the data breach in early February 2017 and notified the Ministry of Education two days later. There are however a number of possible reasons for the delay which would explain the discrepancy in the case number, chief amongst which might be PDPC choosing to initiate investigations at a later date only once it became apparent that there might be grounds for investigation.

[43] *Re Amicus Solutions Pte Ltd and anor* [2019] SGPDPC 33

[44] *Re Dimsum Property Pte Ltd* [2018] SGPDPC 20

[45] Kaspersky, "Ransomware by the numbers: Reassessing the threat's global impact" *Securelist by Kaspersky* (23 April 2021) <https://securelist.com/ransomware-by-the-numbers-reassessing-the-threats-global-impact/101965/> (accessed 21 September 2021)

[46] See e.g. Joseph Johnson, "Annual number of ransomware attacks worldwide from 2016 to 2020", *statista* <https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/> (accessed 21 September 2021)

[47] Given the likely delays to PDPC's investigation timeline caused by the COVID-19 pandemic (see text accompanying *supra* note **Error! Bookmark not defined.**), the small number of cases in 2021 renders it unreliable as an indicator of any general trends in cybersecurity and data protection.

[48] For instance, the PDPC released 49 grounds of decision in 2019, but received approximately 3,500 complaints over the whole year: <https://www.pdpc.gov.sg/help-and-resources/2020/04/enquiry-and-complaint-figures> (accessed 21 September 2021)

[49] Even prior to the 2020 amendments to the PDPA which created an obligation to report data breaches, many data organisations were already informing the PDPC about data breaches of their own accord. Within the dataset of 144 grounds of decision, at least 33 originated solely from voluntary notifications by the data organisation, with 5 others involving both voluntary notifications by the data organisation and complaints by individual members of the public.

[50] Guide to Active Enforcement, p5-6

> "The scope of the PDPA is wide. Consequently, not all complaints and incidents can be investigated. This guide on the Active Enforcement Framework… reiterates the PDPC's general approach to maximise the use of facilitation and mediation in seeking a resolution between the complainant and the organisation concerned. Notwithstanding, the PDPC will not hesitate to send a clear message of wrongdoing where necessary." (emphasis added)

What the PDPC considers a necessary occasion to send a clear message of wrongdoing appears to be linked to data protection incidents "with **high impact**"[51] (bolding in original). Conversely, the PDPC also has the discretion to suspend or discontinue investigations into potential breaches of the PDPA where the impact is assessed to be low.[52]

As for the publications of decisions, while the Personal Data Protection (Enforcement) Regulations 2021 leave it to the PDPC's discretion about whether to publish grounds of decisions,[53] and although the PDPC itself also states that the publication of decisions is at its discretion,[54] it appears to be the PDPC's policy generally to publish grounds of decision in the interests of transparency and public education.[55] The combined effect of the PDPC choosing to pursue investigations in higher-impact data breaches, and the general publication of decisions where its investigations disclose data breaches, suggests that the cases featured in the PDPC decisions fall on the more egregious side of the scale in terms of data breaches – if not necessarily in terms of the impact of the data breach itself, then in the manner of breach relative to general expectations for data protection.

It is also possible that cybersecurity cases form such a large proportion of cases in 2020 because the Protection Obligation to which they relate is the only one of the nine pre-2020 data protection obligations to be a persistently active obligation, compliance with which requires regular action by the data organisation, and therefore the only one that can be constantly breached through mere inaction, raising the chances of the breach actually being detected. The nine pre-2020 data protection obligations are as follows:[56]

- Accountability (ss 11-12 PDPA)
- Notification (s20 PDPA)
- Consent (ss13-17 PDPA)
- Purpose Limitation (s18 PDPA)
- Accuracy (s23 PDPA)
- Protection (s24 PDPA)
- Retention Limitation (s25 PDPA)
- Transfer Limitation (s26 PDPA)
- Access and Correction (ss21-22 PDPA)

[51] Guide to Active Enforcement, p25.

[52] Guide to Active Enforcement, p12. See also PDPC, *PDP Digest 2017*, where a large number of case summaries were published in which the PDPC discontinued investigations as no data breach was disclosed. See also *Re My Digital Lock* [2018] SGPDPC 3 where investigations were discontinued as the PDPC deemed that the central issue in the case was not fundamentally one of data protection.

[53] r 15, PDP (Enforcement) Regulations, No. S 62/2021

[54] Guide to Active Enforcement, p7

[55] PDPC, Advisory Guidelines on Enforcement of DP Provisions (rec 1 Feb 2021), para 28.4.1 <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-Enforcement-of-DP-Provisions-1-Feb-2021.pdf?la=en>. This policy has been in place since the first iteration of the PDPC Enforcement regulations: Advisory Guidelines (ver 21 April 2016), para 26.4.1.

[56] See PDPC, "Data Protection Obligations" <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act/Data-Protection-Obligations> (accessed 21 September 2021)

It is arguable that other than the Protection Obligation, every other obligation can either be fulfilled with relatively "one-off" actions, or is only triggered on the occurrence of specific events. The Accountability, Notification, Consent, and Purpose Limitation obligations (hereinafter the "one-off obligations") can be generally fulfilled by the creation of an appropriate policy for the collection, use, and disclosure of personal data which is then made known to persons from whom personal data is collected, and which does not generally need too much updating on a regular basis. The Accuracy, Access and Correction, Retention Limitation and Transfer Limitation Obligations (hereinafter the "triggered obligations") are generally triggered only on the occurrence of specific events, such as a request by an individual regarding his personal data, or the active transfer of personal data across borders.

Given that the PDPA has been enforced for at least 7 years since 2 July 2014,[57] it is likely that the proportion of organisations which are still not in compliance with the one-off obligations has dwindled over time as a result of the PDPC's outreach and enforcement efforts. As such, the number of cases dealing with one-off obligations would also naturally fall over time. The following table, showing the number of cases dealing with only one-off obligations since 2016, seems to bear out this assertion (disregarding 2021, which has an extremely small base of 4 published cases within the dataset).

[57] See PDPC, "PDPA Overview" <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act> (accessed 21 September 2021)

Year	Number (% of total cases)	Cases
2016	5 (22.7%)	*Re Yestuition Agency,*[58] *Re AIA Singapore Private Limited,*[59] *Re Chua Yong Boon Justin,*[60] *Re Comfort Transportation and anor,*[61] *Re Jump Rope (Singapore)*[62]
2017	2 (10.5%)	*Re Exceltec Property Management Pte Ltd and ors,*[63] *Re M Stars Movers & Logistics Specialist Pte Ltd*[64]
2018	8 (27.5%)	*Re Sharon Assya Qadriyah Tang,*[65] *Re Jiwon Hair Salon and ors,*[66] *Re Actxa Pte Ltd,*[67] *Re Aventis School of Management Pte Ltd,*[68] *Re MyRepublic Limited,*[69] *Re Spring College International Pte Ltd,*[70] *Re Club the Chambers,*[71] *Re Big Bubble Centre*[72]
2019	8 (16.3%)	*Re German European School Singapore,*[73] *Re H3 Leasing,*[74] *Re Starhub Mobile Pte Ltd and ors,*[75] *Re Skinny's Lounge,*[76] *Re Xbot Pte Ltd,*[77] *Re AgcDesign Pte Ltd,*[78] *Re ChampionTutor Inc,*[79] *Re Amicus Solutions Pte Ltd and anor*[80]
2020	1 (4.8%)	*Re Majestic Debt Recovery*[81]
2021	1 (25%)	*Re Progressive Builders Private Limited and anor*[82]

Table 4: Breaches of the one-off obligations by year

As for the triggered obligations, these have generally been very rare; only 10 unique cases have involved any of the triggered obligations out of a total of 144 grounds of decisions.[83]

[58] [2016] SGPDPC 5

[59] [2016] SGPDPC 10

[60] [2016[SGPDPC 13

[61] [2016] SGPDPC 17

[62] [2016] SGPDPC 21

[63] [2017] SGPDPC 8

[64] [2017] SGPDPC 15

[65] [2018] SGPDPC 1

[66] [2018] SGPDPC 2

[67] [2018] SGPDPC 5

[68] [2018] SGPDPC 7

[69] [2018] SGPDPC 13

[70] [2018] SGPDPC 15

[71] [2018] SGPDPC 24

[72] [2018] SGPDPC 25

[73] [2019] SGPDPC 8

[74] [2019] SGPDPC 9

[75] [2019] SGPDPC 12

[76] [2019] SGPDPC 13

[77] [2019] SGPDPC 19

[78] [2019] SGPDPC 23

[79] [2019] SGPDPC 25

[80] [2019] SGPDPC 33

[81] [2020] SGPDPC 7

[82] [2021] SGPDPC 2

[83] The breakdown is as follows:

- Access and Correction: 1 case (*Re Management Corporation Strata Title Plan No 4436* [2018] SGPDPC 18)
- Accuracy: 1 case (*Re Credit Bureau (Singapore) Pte Ltd* [2018] SGPDPC 14)

The combined effect of breaches of the one-off obligation dwindling, and the relative rarity of the triggered obligations, suggests that the proportion of PDPC cases that deal with the Protection Obligation will rise over time. Unfortunately, the disruption to the PDPC's processes caused by the COVID-19 pandemic means that there are insufficient data points in 2021 to confirm this trend at this time of writing.

Specific trends

Voluntary notification

In general, there is a significant rate of voluntary notification (even before the 2020 amendments to the PDPA that created the Data Breach Notification Obligation):[84] out of 144 grounds of decision, the breaching data organisation voluntarily notified the PDPC in 38 grounds of decision, or about 26% of the time.

It must be noted that voluntary notification is a mitigating factor in terms of any financial penalty subsequently imposed on the data organisation,[85] which was explicitly noted by the PDPC as early as in *Re Central Depository (Pte) Ltd and anor*.[86] This is a significant confounding factor, as it directly informs data organisations' approaches towards dealing with a data breach, which is to attempt to mitigate the impact of any regulatory action by the PDPC via voluntary notification.

This is in contrast to other, "organic", factors, such as the means by which the data organisation comes to find out about the data breach. In many cases, inadvertent disclosure of personal data online is only discovered by someone coming across personal data, whether or not their own, that has been leaked.[87] Whether or not the data organisation has an opportunity to notify the PDPC also depends on whether or not the individual would prefer to approach the data organisation directly to resolve their concerns over a data breach involving their personal data[88] or instead approach the PDPC directly,[89] or both.[90]

Profiling the data organisations involved, including such attributes as their entity size, brand recognition, and level of consumer trust enjoyed, to determine whether individuals would prefer to go to them to resolve privacy concerns is beyond the scope of this paper. It does, however, raise the possibility that voluntary notification may not always be a breaching data organisation's choice to make, and therefore access to voluntary notification as a mitigating factor may in practice simply not be available to a segment of commercial enterprises. In any case, it is also partially moot as the PDPA

- Retention Limitation: 6 cases (*Re Social Metric Pte Ltd* [2017] SGPDPC 17, *Re Credit Bureau (Singapore) Pte Ltd* [2018] SGPDPC 14, *Re O2 Advertising Pte Ltd* [2019] SGPDPC 32, *Re MSIG Insurance (Singapore) Pte Ltd and anor* [2019] SGPDPC 43, *Re Singapore Red Cross Society* [2020] SGPDPC 16, and *Re Times Software Pte Ltd and ors* [2020] SGPDPC 18)
- Transfer Limitation: 3 cases (*Re Bud Cosmetics* [2019] SGPDPC 1, *Re Spize Concepts Pte Ltd* [2019] SGPDPC 22, and *Re Singapore Technologies Engineering Limited* [2020] SGPDPC 21)

[84] Part VIA of the *Personal Data Protection Act 2012* (No 26 of 2012, Sing), as amended by the *Personal Data Protection (Amendment) Act 2020* (No 40 of 2020, Sing)

[85] PDPC, Guide to Active Enforcement at p28 <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-on-Active-Enforcement-15-Mar-2021.pdf?la=en> (hereinafter "Guide to Active Enforcement")

[86] [2016] SGPDPC 11 at [24(d)]

[87] See e.g. *Re K Box Entertainment Group Pte Ltd and anor* [2016] SGPDPC 1, *Re Fei Fah Medical Manufacturing Pte Ltd* [2016] SGPDPC 3, *Re Propnex Realty Pte Ltd* [2017] SGPDPC 1, *Re WTS Automotive Services Pte Ltd* [2018] SGPDPC 26, and *Re O2 Advertising Pte Ltd* [2019] SGPDPC 32.

[88] See e.g. *Re MSIG Insurance (Singapore) and anor* [2019] SGPDPC 43

[89] See e.g. *Re Bud Cosmetics* [2019] SGPDPC 1

[90] See e.g. *Re InfoCorp Technologies Pte Ltd* [2019] SGPDPC 17

now contains a data breach notification requirement, so the fact that there is now a duty on a data organisation to report a notifiable data breach must detract from the value of voluntary notification as a mitigating factor.[91]

Cybersecurity

Of the 144 PDPC decisions, 27 cases were classed as "NA", meaning that only the remaining 117 out of 144 grounds of decisions involved the Protection Obligation. Of these 118 grounds of decisions that involved the Protection Obligation, 72 were classified as bearing cybersecurity aspects, and 45 were classified as not bearing cybersecurity aspects. A further breakdown of cases involving cybersecurity by year follows:

Year	Total Cases	Cases involving cybersecurity (% of total cases)	Deliberate hacks (% of cybersecurity cases)	Online exposure (% of cybersecurity cases)
2016	22	9 (40.9%)	4 (44.4%)	5 (55.6%)
2017[92]	19	8 (42.1%)	1 (12.5%)	6 (75.0%)
2018	29	9 (27.6%)	0 (0%)	9 (100%)
2019[93]	49	27 (55.1%)	8 (29.6%)	18 (66.7%)
2020	21	16 (76.2%)	6 (37.5%)	10 (62.5%)
2021 – to date[94]	4	2 (50.0%)	1 (50.0%)	1 (50.0%)

Table 1: PDPC decisions involving cybersecurity by year.

Other than in 2018, a significant percentage of grounds of decisions issued each year deal with cybersecurity, reaching a maximum of over 75 percent of cases dealing with cybersecurity in 2020.

In terms of the impact of the data breaches involved, it is only possible to quantify the data breaches in 122 cases, as only in those cases were known quantities of exposed personal data specified in the grounds of decision. 112 of these cases specified at least the amount of breached personal data, with a further 10 cases specifying only the amount of vulnerable personal data. Given the relatively few cases (27 out of 144) that state the amount of vulnerable personal data, and the difficulty in distinguishing breached personal data and vulnerable personal data, the remainder of the analysis in this section proceeds solely on the basis of the amount of breached personal data.

Some notable statistics on the amounts of breached personal data follow:

[91] See e.g. *Public Prosecutor v Sakthikanesh s/o Chidambaram and ors* [2017] 5 SLR 707 at [55], and *Public Prosecutor v Leong Sow Hon* [2019] SGMC 42 at [21].

[92] The discrepancy of one case is due to *Re BHG (Singapore) Pte Ltd* [2017] SGPDPC 16, which facts involved a data subject mis-entering his particulars into a page that already partially contained the personal data of another person.

[93] The discrepancy of one case is due to *Re The Travel Corporation (2011) Pte Ltd* [2019] SGPDPC 42, which facts involved the loss of a hard disk containing personal data. See also *supra* note 27.

[94] The last ground of decision captured in the dataset was *Re HMI Institute of Health Sciences Pte Ltd* [2021] SGPDPC 4.

	Total	Cybersecurity cases	Non-cybersecurity cases
Number of cases	112	57	55
Maximum	1,500,000[95]	1,500,000	165,306[96]
Minimum	0[97]	0	1
Mean	34,363	61,271	6,477
Median	132	405	8
Mode	1	384	1

Table 2: Volume of breached personal data by case type

It appears that the volume of personal data breached in cybersecurity cases is at least an entire order of magnitude apart from the volume of personal data breached in non-cybersecurity cases. However, this is before accounting for the outlier that is *Re Singapore Health Services Pte Ltd and anor* ("*Re SingHealth*"),[98] the single largest data breach in Singapore history, and itself an entire order of magnitude larger than the next largest data breaches.[99] Furthermore, given that *Re SingHealth* involved a deliberate and systematic hack of the data organisation's electronic patient health records by an advanced persistent threat actor,[100] it is arguable that *Re SingHealth* is highly atypical and not representative of the average data breach involving cybersecurity aspects.

For that reason, it may be more apt to re-examine the statistics on the volume of breached personal data, excluding *Re SingHealth*:

	Total	Cybersecurity cases	Non-cybersecurity cases
Number of cases	111	56	55
Maximum	484,512[101]	484,512	165,306
Minimum	0	0	1
Mean	21,159	35,579	6,477
Median	128	394.5	8
Mode	1	384	1

Table 3: Volume of breached personal data by case type, excluding *Re SingHealth*

While the mean of breached personal data across all cases, as well as cybersecurity cases, falls as a result of the exclusion of *Re SingHealth*, the relative disparity between cybersecurity cases and non-cybersecurity cases remains. Given the large volume of breached personal data at the top end, the median is more indicative than the mean of the "average" case of its type; this indicates that roughly 400 sets of personal data are breached in cybersecurity cases compared to only 8 in non-cybersecurity cases.

It should be unsurprising that the volume of personal data breached is higher across the board in cybersecurity cases. Many of the data breaches involved in cybersecurity cases involve actual or

[95] *Re Singapore Health Services Pte Ltd and anor* [2019] SGPDPC 3

[96] *Re Challenger Technologies Limited and anor* [2016] SGPDPC 6

[97] *Re Singapore Management University Alumni Association* [2018] SGPDPC 6

[98] [2019] SGPDPC 3

[99] The next five data breaches after *Re SingHealth* involved hundreds of thousands of personal data sets, from 484,512 in *Re Creative Technology Ltd* [2020] SGPDPC 1 to 250,328 in *Re Marshall Cavendish Education Pte Ltd* [2019] SGPDPC 34.

[100] *Re Singapore Health Services Pte Ltd and anor* [2019] SGPDPC 3 at [98]

[101] *Re Creative Technology Ltd* [2020] SGPDPC 1

potential wholesale access to databases or records,[102] which would automatically increase the amount of personal data reckoned by the PDPC to have been part of the data breach if the entire database was at risk. In contrast, only the top two non-cybersecurity cases by volume of personal data breached reached 6-digit figures, and were related to e-mailing errors.[103] Many other non-cybersecurity cases related to limited physical disclosure of data, or physical mailing errors, which nature would limit the amount of personal data breached.

Reasonable security measures

Moving on to the analysis of reasonable security measures in the context of cybersecurity, there are very few cases where the PDPC have found that an organisation has taken reasonable security measures in spite of a data breach having occurred.

184 organisations (whether data organisations or data intermediaries) were named as subjects of PDPC investigations in the 144 grounds of decisions. Out of these 184 organisations, 143 were investigated for potential breaches of the Protection Obligation, and out of these 143 investigation subjects, only 19 of them were found to not have breached the Protection Obligation. And of these 19 organisations that did not breach the Protection Obligation, 15 of them were involved in 11 grounds of decisions where a finding of breach of the Protection Obligation was made against another organisation which was also a subject of investigation.

These 11 grounds of decision can be classified into two archetypes. The first is where a data organisation had outsourced data processing to a data intermediary, and where the actual data breach was committed by the data intermediary. In such cases, the data organisation was absolved because of the contractual or operational arrangements it had made with the data intermediary that would hold the data intermediary to a particular standard of data protection. 6 cases make up this first archetype.[104] The second is where the data breach is committed by the data organisation, and the absolved party is a vendor who was found, on the facts, not to have been a data intermediary of the data organisation because they merely handled infrastructural as opposed to data processing aspects of the data organisation's business, and therefore to whom data protection obligations did not attach. 5 cases make up this second archetype.[105] As such, none of these 11 grounds of decision are necessarily instructive in terms of the actual technical measures needed to meet the standard of reasonable security in the Protection Obligation.

Only in 4 grounds of decisions – *Re BHG (Singapore) Pte Ltd* ("*Re BHG*"),[106] *Re Cigna Europe Insurance Company SA NV* ("*Re Cigna*"),[107] *Re Executive Link Services Pte Ltd* ("*Re ELS*"),[108] and *Re Singapore*

[102] See e.g. *Re Learnaholic Pte Ltd* [2019] SGPDPC 31, *Re Watami Food Service Singapore Pte Ltd* [2018] SGPDPC 12

[103] *Re Challenger Technologies Limited and anor* [2016] SGPDPC 6 (165,306 personal data sets breached) and *Re GrabCar Pte Ltd* [2019] SGPDPC 15 (120,747 personal data sets breached)

[104] *Re Central Depository (Pte) Limited and anor* [2016] SGPDPC 11, *Re Aviva Ltd and anor* [2016] SGPDPC 15, *Re Singapore Telecommunications Limited and anor* [2017] SGPDPC 4, *Re Tiger Airways Singapore Pte Ltd and ors* [2017] SGPDPC 6, *Re AIG Asia Pacific Insurance Pte Ltd and anor* [2019] SGPDPC 2, *Re Times Software Pte Ltd and ors* [2020] SGPDPC 18

[105] *Re Smiling Orchid and ors* [2016] SGPDPC 19, *Re Singapore Cricket Association and anor* [2018] SGPDPC 19, *Re Management Corporation Strata Title Plan No 4375 and ors* [2020] SGPDPC 4, *Re Management Corporation Strata Title Plan No 3593 and ors* [2020] SGPDPC 6

[106] [2017] SGPDPC 16

[107] [2019] SGPDPC 18

[108] [2019] SGPDPC 30

Telecommunications Limited ("*Re Singtel (2020/13)*")[109] – were there no findings of breach of the Protection Obligation against the organisation investigated. These four grounds of decisions are somewhat illuminating as to the cybersecurity measures that organisations should take to meet a reasonable standard of protection, but a closer examination discloses some concerns and possible loopholes in the PDPA's data protection regime.

Two cases arguably do not involve cybersecurity to an appreciable degree. In *Re Cigna*, the data organisation was absolved of a breach of the Protection Obligation because it had outsourced the data processing to a related UK entity within the Cigna group, which was obligated to act by the Cigna group's internal policies relating to data protection. Because the UK entity was beyond the PDPC's jurisdiction, the PDPC could only restrict itself to examining if the Singapore-based data organisation had sufficiently discharged its data protection obligations as regards inter-jurisdictional transfers.[110] As such, the data organisation's data protection obligations were limited to ensuring that its data intermediary complied with a standard of data protection comparable to that under the PDPA, and it is therefore closer on the facts to the first archetype of cases where the data intermediary but not the data organisation is found in breach of the Protection Obligation.

In *Re BHG*, the internal policies and procedures of the data organisation were disrupted by a combination of unplanned technical faults and the inexplicable failure of both a staff member to perform a simple refresh (which had been done without incident for most of that workday) as well as a customer who entered his personal data into someone else's partially completed form. The actions of the customer who mistakenly entered his personal data into the partially completed form were "one of the baffling features of [the] case".[111] It could be argued that the actions of this unknown customer were a *novus actus interveniens* that made it unjust to attach blame entirely to the data organisation.

While *Re ELS* and *Re Singtel (2020/13)* both involved cybersecurity, both were arguably cases where outsourcing saved the organisation from a finding of breach. In *Re ELS*, the data organisation had engaged two IT vendors (who were not direct subjects of the PDPC investigation) to run its IT operations, and they had enabled an urgent VPN workaround on a remote internal server because of a glitch affecting the data organisation's operations. That workaround permitted the data breach in question to occur.

Two aspects of the case ultimately informed the PDPC's decision to find the data organisation not in breach. First, it found that the data was leaked from an internal server which was never configured to be publicly accessible,[112] and the data breach in question only happened because the VPN workaround created a vulnerability in that server which enabled the data to become publicly accessible. Second, the PDPC found that, in view of the urgency of the fix that created the vulnerability, the data organisation was entitled to the operating assumption that its vendors had not materially compromised its security (and hence its data protection) by implementing that fix. Moreover, the data organisation had specifically engaged its vendors for their IT and security expertise which it impliedly did not have. Therefore, even if the data organisation had specifically asked about security, it may well

[109] [2020] SGPDPC 13. As Singtel is also the subject of a case summary that will be discussed later, the year and neutral citation number are added as a disambiguator.

[110] *Supra* note 1 at s26.

[111] *Re BHG* at [22(c)]

[112] In contrast to public-facing servers hosting webpages, accessible through the Internet, for which data would be publicly available by default in the absence of appropriate configurations. The vast majority of PDPC decisions involving inadvertent online exposure of data involve public-facing servers rather than the internal server that was in fact exposed in this case.

have received an answer that the fix in fact deployed was adequate in terms of cybersecurity, and would not necessarily have had the internal expertise to question the expert advice of its vendors.

In *Re Singtel (2020/13)*, the data organisation's vendor omitted to report a code change in its mobile app as ordinarily required by an agreed operating protocol, resulting in the data organisation not being aware that conducting testing to detect any adverse effects of the change was even needed. As such, the data breach occurred without the data organisation having an opportunity to even detect the glitch. The PDPC stated that the tests that were ordinarily conducted on the mobile app were "reasonably scoped" to pick up errors and flaws prior to development, which implies that the technical measures that were in fact implemented in this case were considered to be reasonable.

Both *Re ELS* and *Re Singtel (2020/13)* are somewhat instructive as to the technical measures to be taken that will be considered reasonable under the PDPA. *Re ELS* featured reliance on external cybersecurity advice; this is the obvious improvement over simply neglecting cybersecurity if cybersecurity expertise is not readily available within the data organisation, which would otherwise lead to a breach of the Protection Obligation.[113] *Re Singtel (2020/13)* featured comprehensive descriptions of a two-pronged data protection policy put in place by the data organisation: not only did the data organisation take it upon itself to ensure that its vendors' employees were fully apprised of cybersecurity concerns and that its vendors' data protection arrangements were verified, the data organisation also implemented *reasonably scoped* pre-launch tests for code changes. This is to be contrasted against relatively piecemeal testing which might not be appropriately scoped to cover all personal data held by the data organisation,[114] or which only test for business functionality but not with data protection concerns in mind.[115]

In addition to the four grounds of decisions canvassed above, it is worth mentioning three other PDPC decisions that have a bearing on what the PDPC considers to be reasonable cybersecurity measures: *Re ComGateway (S) Pte Ltd* ("*Re ComGateway*"),[116] *Re InfoCorp Technologies Pte Ltd* ("*Re InfoCorp*"),[117] and a case summary, *Re Singapore Telecommunications Limited* ("*Re Singtel (12 August)*").[118]

In *Re InfoCorp*, the data organisation was gathering personal data for a cryptocurrency registration exercise, which included collecting personal data as well as know-your-customer documents ("KYC documents") as part of prevailing anti-money laundering/countering terrorist financing measures. In relation to the personal data that was directly collected, the PDPC found that "[e]ncryption of the Personal Data Sets had prevented unauthorised access by third parties", and therefore that reasonable security arrangements had been made.[119] However, the KYC documents were not encrypted and were issued a serialised file identity, which was incorporated into the URL used to access them; combined with the lack of any authentication mechanisms, this meant that registrants

[113] See e.g. *Re Smiling Orchid and ors* [2016] SGPDPC 19 and *Re Tutor City* [2019] SGPDPC 5

[114] see e.g. *Re InfoCorp Technologies Pte Ltd* [2019] SGPDPC 17, where the data organisation had adequate security measures and some testing in relation to its primary personal data sets held, but not the documents that authenticated these primary personal data sets and were in and of themselves personal data.

[115] See e.g. *Re Funding Societies Pte Ltd* [2018] SGPDPC 29 at [27], where the data organisation claimed that it conducted testing on their website, but subsequently qualified this to state that they had focused on functionality and load testing rather than security and protection.

[116] [2017] SGPDPC 19

[117] [2019] SGPDPC 17

[118] *Re Singapore Telecommunications Limited* (12 August 2021), DP-2007-B6607.

[119] Encryption is to be distinguished from encoding, which is relatively easily reversible (see *Re ComGateway (S) Pte Ltd* [2017] SGPDPC 19 at [27]), and hashing, which is one-way encryption for which security depends on the precise algorithm used (see *Re Creative Technology Ltd* [2020] SGPDPC 1 at [11]).

could manipulate their provided URL to access the KYC documents of other registrants, ultimately leading to the finding of breach in the case.

In *Re Singtel (12 August)*, despite the compromise of some individual personal data held by the data organisation due to a phishing attack, the data organisation's data protection policies were found to be reasonable, including:

- Password requirements in security policies that were aligned to industry best practices;
- Continual network and system enhancements to improve application and infrastructure security;
- Comprehensive annual mandatory training for staff; and
- Reasonable security measures in place for the work environment.

Unfortunately, for security reasons, the PDPC does not further delve into the specific measures that were taken, but the measures outlined above give a fairly comprehensive view of what a general cybersecurity posture should look like for a major data organisation[120] to be considered to have made reasonable security measurements.

In *Re ComGateway*, two separate data breaches were at issue. The data organisation was found to have sufficiently discharged its data protection obligations only in respect of one data breach. The data breach for which the data organisation was found liable was a URL manipulation vulnerability, which is not uncommon amongst cybersecurity-related breaches of the Protection Obligation.[121]

The data breach for which the data organisation was not found liable was found to be an irreproducible glitch. The personal data of the complainant was inadvertently accessed by another customer, B, of the data organisation, when B accessed the shipping webpage run by the data organisation. The data organisation had in place a fairly robust IT security framework, including the use of quarterly vulnerability scans, annual penetration tests, managed firewall applications, and automated code checks. When the glitch was brought to its attention, code and log reviews, as well as tests aimed at reproducing the glitch, were all unsuccessful in determining the cause of the glitch. The PDPC ultimately found that despite this data breach, the irreproducible nature of the glitch, combined with evidence of a robust cybersecurity posture, meant that the data organisation's security arrangements were reasonable.

Combined, all the above cases provide some insights into what reasonable cybersecurity measures would look like. *Re ComGateway*, *Re Singtel (12 August)* and *Re Singtel (2020/13)* all suggest that defence in depth is viewed very favourably, combining multiple security measures to reduce the risk of a single point of failure. *Re BHG*, *Re Singtel (12 August)* and *Re Singtel (2020/13)* highlight the importance of not neglecting the human aspect of cybersecurity, by ensuring that staff are trained well and that there is proof that they are generally able to perform their duties as trained. And *Re ELS* emphasises the need to engage the necessary cybersecurity expertise if the same is lacking from within the organisation. In addition, the PDPC has also very recently released two new guides

[120] The data organisation in question is Singtel, one of the three largest telecommunications companies in Singapore. Compare and contrast *Re Singapore Health Services Pte Ltd and anor* [2019] SGPDPC 3, where despite the data organisation having a similarly-scoped suite of data protection policies, its actual implementation of them fell drastically short, resulting in a finding of breach of the Protection Obligation.

[121] See e.g. *Re Smiling Orchid and ors* [2016] SGPDPC 19, *Re Fu Kwee Kitchen Catering Services* [2016] SGPDPC 14. See also PDPC, *Guide to Data Protection Practices for ICT Systems* at p19.

pertaining specifically to cybersecurity: the “Guide to Data Protection Practices for ICT Systems”[122], and “How to Guard Against Common Types of Data Breaches?”;[123] competent implementation of the security measures in these guides, alongside advice from prior PDPC guides and advisory guidelines, should go a long way towards supporting a finding that security arrangements were reasonable in the event of a breach.[124]

A lacuna in the PDPA?

Despite the measures that the data organisations took in *Re ELS* and *Re Singtel (2020/13)* that were considered to be reasonable under the circumstances, their factual circumstances also make clear a lacuna in the PDPA as far as the definitions of “reasonable security measures” and “data intermediary” are concerned.

In short, a vendor that is responsible exclusively for IT infrastructure and does not process data on behalf of a data organisation, and which does something that adversely affects a data organisation’s cybersecurity posture and data protection measures (whether deliberately or by accident), will not be responsible in any way for any data breach that results from that adverse action, as it was not considered to be a data intermediary of the data organisation.[125]

This was made clear in *Re Civil Service Club*,[126] where the PDPC explicitly noted that while a vendor’s work scope did not involve processing of any personal data on behalf of the data organisation, and therefore was not a data intermediary that would share in the data organisation’s Protection Obligation, it was nonetheless in a position to either handle personal data incidentally, or make software system design decisions that would affect the security of the personal data held by the data organisation. In that case, the data organisation was held liable for a failure to clearly articulate its data protection requirements to its vendor and to make data protection clauses part of its service contract with the vendor.

However, the corollary of *Re Civil Service Club* is that if the data organisation has in fact articulated its data protection requirements to its vendor and made cybersecurity and data protection part of the ambit of the contract of service with the vendor, then the data organisation will have adequately discharged its Protection Obligation, even if the vendor subsequently renders bad advice or otherwise compromises the cybersecurity and data protection posture of the data organisation.

This means that there can be a breach of cybersecurity for which fault can be assigned (namely the vendor which should have known better, or which might have been negligent in taking actions detrimental to the cybersecurity and data protection posture of the data organisation), but for which liability for a data breach cannot be brought home because of the overly restrictive definition of a data

[122] PDPC, Guide to Data Protection Practices for ICT Systems <https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/Tech-Omnibus/Guide-to-Data-Protection-Practices-for-ICT-Systems.pdf?la=en>

[123] PDPC, How to Guard against Common Types of Data Breaches? <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/tech-omnibus/how-to-guard-against-common-types-of-data-breaches-handbook.pdf>

[124] See e.g. *Re Singapore Telecommunications Ltd* [2020] SGPDPC 13 at fn4, where the PDPC’s Guide on Building Websites for SMEs was referenced when commenting on the data organisation’s good practice of making personal data protection part of the contractual terms with its vendor. Cf *Re Civil Service Club* [2020] SGPDPC 15 at fn3, where the same guide was referenced to point out what the data organisation could have done better in designing its website in terms of personal data protection.

[125] See text accompanying *supra* note 105.

[126] [2020] SGPDPC 15 at [10]-[13]

intermediary, which must process data on behalf of a data organisation in order for data protection obligations to attach. A comparison with one previous PDPC decision, *Re Singapore Telecommunications Limited* ("*Re Singtel (2017/4)*"),[127] reveals how this characterisation can be essentially arbitrary.

The facts of *Re Singtel (2017/4)* are surprisingly similar to that of *Re Singtel (2020/13)*. The data organisation had engaged a third-party contractor to assist it with some of its business functions. In both cases, the data organisation had clear policies and procedures in place to satisfy itself that its contractor complied with the PDPA. A code defect combined with a breach of the pre-established protocols resulted in the data breach under investigation.

In *Re Singtel (2017/4)*, the third-party contractor had been granted access to a personal data database as part of its services to maintain the data organisation's app. This access to personal data was sufficient to characterise the third-party contractor as a data intermediary, to whom data protection obligations now applied in full, and whose carelessness and breach of pre-established protocols combined to render it in breach of the Protection Obligation. In contrast, in *Re Singtel (2020/13)*, the third-party contractor's functions were restricted to code development for that same app – which included code that processed personal data[128] – and as such was not found to be a data intermediary.[129]

The line that differentiates a vendor dealing with code that affects personal data, and a data intermediary that actually processes personal data, therefore seems to be an exceedingly fine one. The difference would appear to hinge on whether or not a data organisation requires a data intermediary to process data on its behalf or not, which might well be decided by business exigency rather than out of any data protection concerns. From the point of view of personal data protection in general, such a distinction between a vendor and a data intermediary goes against the whole point of data protection by design, where personal data is protected by more than just measures dealing with its collection, use, and disclosure, but also by a careful consideration of the degree of its integration into an organisation's business needs.[130]

It could well be argued that it is overly onerous for a vendor to be apprised of how its work fits into its principal's data protection posture in general. However, given that a vendor has to be informed in broad strokes of how its deliverables fit within the scope of its principal's own operations, it ought not be too far a stretch for the vendor to be informed of the data protection implications arising from its work. As it is, the PDPC already considers it reasonable for a data organisation to inform a vendor of detailed requirements and specifications, especially as part of its own data protection obligations,[131]

[127] [2017] SGPDPC 4

[128] In this case, code that decoupled (hence organising or altering, under limb (c) of the definition of processing under s2 PDPA) recycled mobile numbers (itself a type of personal data – see *Re Singtel (2020/13)* at [6(a)]) from previous users.

[129] *Re Singtel (2020/13)* at [9].

[130] See PDPC, Guide to Data Protection by Design for ICT Systems (31 May 2019) < https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Protection-by-Design-for-ICT-Systems-(310519).pdf?la=en> (accessed 21 September 2021). This guide has since been superseded by the Guide to Data Protection Practices for ICT Systems, which does not specifically reference data protection by design, but does emphasise the importance of design considerations in selecting network and database configurations, among other things.

[131] See e.g. *Re Singapore Cricket Association and anor* [2018] SGPDPC 19 at [23] and *Re Central Depository (Pte) Limited & anor* [2019] SGPDPC 24 at [40].

and some organisations even take it upon themselves to ensure that their vendors are briefed on personal data protection.[132]

It is also arguable that any negligence in a vendor's work should be a matter between itself and its principal. This may well be true when the principal is found to be in breach of a data protection obligation itself due to the fault of its vendors, and recourse may be had to indemnity clauses. But if the vendor's negligence has led to a data breach, then whether or not the principal is itself in breach of any data protection obligations, damage to the individuals whose personal data was breached has still resulted in the form of the disclosure of their data, which will not be within the scope of any indemnity between the vendor and the principal. Given that the entire point of the PDPA was to ensure some degree of protection for individuals' personal data, permitting a lackadaisical vendor to escape public or administrative sanction appears counterproductive to the general aim of raising personal data protection awareness amongst organisations. The solution may lie in a more expansive interpretation of an intermediary,[133] but that implies a rather fundamental rework of Singapore's data protection regime.

Conclusion

The PDPC's increasing focus on cybersecurity – or rather the increasing prominence of cybersecurity in personal data protection – was bound to happen sooner or later as data protection enforcement shifts to focus on data protection in a digitalised world. To its credit, despite cybersecurity not being explicitly within its ambit, the PDPC has done its part to educate organisations on the role that cybersecurity has to play in data protection with the release of several guides, and between those guides and the PDPC cases released for public education, it is possible to elucidate a reasonable standard of cybersecurity that data organisations should implement. The key appears to be a well-rounded cybersecurity posture, with at the minimum the use of firewalls, robust account policies, and some degree of security or vulnerability testing, combined with staff training and supervision to ensure at least some awareness of data protection.

However, advancements in technologies like platform or software as a service, increases in digital threats like hacks and ransomware attacks, as well as changes to how organisations engage services that have a bearing, however indirect, on data protection, portend significant changes in data protection paradigms compared to when the PDPA was first enacted. In particular, while the PDPA's emphasis on possession and control over personal data is understandable as a touchstone for determining upon whom to impose data protection obligations, the vendor lacuna identified in *Re ELS* and *Re Singtel (2020/13)* suggests that data protection is not contingent only on organisations which have possession and control over personal data, and that vendors which are not deemed to be data intermediaries may nonetheless have outsize impacts on the cybersecurity – and hence data protection – postures of their principals. It runs counter to data protection in general if such vendors are not made aware of the implications of their actions, and the easiest way to do that would be to impose new data protection obligations.

Yet considering that personal data protection has to strike a balance between individual protection and the commercial interests of businesses, it is not clear that the imposition of more regulations is a good thing. At the very least, it further raises compliance costs, and possibly also barriers to entry, of organisations that aim to harness cloud software services as an accelerator for their business, if they

[132] *Re Singtel (2020/13)* at [12(a)].

[133] See Daniel Seng, "Data Intermediaries and Data Breaches" in Simon Chesterman ed, *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World*, 2nd ed, (Singapore: Academy Publishing, 2018) at 7.14

are in no position to dictate terms to these service providers, and lack the necessary technical understanding on their own to be fully cognizant of the data protection implications of the tools they use.

Fortunately, the issue of increasing the scope of organisations who are subject to data protection obligations is not yet pressing. Two cases in recent years do not yet a sea change make. Nonetheless, *Re ELS* and *Re Singtel (2020/13)* should start raising questions about how our current understanding of data protection ought to change in response to technological developments. The primary obligation to protect personal data should remain on the organisation for whose use the data is collected, but cognizance should be taken of a wider suite of supporting actors in keeping that personal data protected.