White Paper on Data Breach Tabletop Exercise

November 2020

By Association of Information Security Professionals

An initiative by AiSP's Cybersecurity Awareness & Advisory Programme and Data & Privacy Special Interest Group

AiSP
Association of Information Security Professionals

About AiSP

Since 2008, the Association of Information Security Professionals (AiSP) is an independent cybersecurity association that believes in developing, supporting and enhancing industry technical competence and management expertise to promote the integrity, status and interests of Information Security professionals in Singapore.

We believe that in promoting the development, increasing and spreading of cybersecurity knowledge can shape more resilient economies.

Our team of passionate volunteers are involved in initiatives and programmes to build and nurture the cybersecurity ecosystem through membership, events, collaboration and knowledge development.

Our Mission

AiSP is the pillar for Information Security Professionals and the overall Information Security Profession through,

- promoting the integrity, recognition and interests of Information Security Professionals in Singapore.
- enhancing technical competence and management expertise in Information Security.
- bolstering the development, increase and spread of information security knowledge and its related subjects.

Our Vision

A safe cyberspace supported by a strong and vibrant cybersecurity ecosystem.

Please connect with us if you want to be part of Singapore's cybersecurity ecosystem today!

AiSP
Advance Connect Excel

About CAAP

Targeted for Singapore SMEs, the **Cybersecurity Awareness and Advisory Programme** (CAAP) aims to drive digital security awareness and readiness. Supported by CSA, our CAAP operating committee focuses on:

- Enhance security awareness and training
- Create cohesive security knowledge resources
- Offer security solutions and services support

The three thrusts are driven by the respective working groups of credible and passionate infosec professionals, supported by AiSP secretariat. We are looking for more companies to tap on CAAP, and more partners and professionals to support the cybersecurity ecosystem.

About Data and Privacy Special Interest Group

AiSP has set up its fourth Special Interest Group (SIG) – Data and Privacy in Sep 2020. Our SIG covers the following topics broadly, with an open view that the emerging trends that should feed into AiSP's Information Security Body of Knowledge and CAAP Body of Knowledge,

- **Data**: Data Analytics, Data Governance, Data Portability, Data Protection, Data Management, Data Security, etc

- **Privacy**: Industry practices and cultural norms of privacy, considerations for using AI, machine learning, tools for automation, etc

SIG aims to enhance current AiSP members' interest in these two broad areas, where our members are in information security and cybersecurity fields. Please contact AiSP Secretariat if you are interested to join.

This tabletop exercise is one of the activities under our Cybersecurity Awareness and Advisory Programme (CAAP), which aims to elevate cybersecurity awareness as integral part of SME business owner's fundamentals.

Background

As Singapore moves into a Smart Nation, companies can gain more business opportunities by adopting a digital business model and using digital tools.

The COVID-19 pandemic has further accelerated the use of digital tools and solutions worldwide, and correspondingly, digital risks as well.

AiSP has been conducting a series of CAAP events together with industry speakers, with the aim to raise cybersecurity awareness among SMEs.

Targeted for Singapore SMEs and supported by the Cyber Security Agency of Singapore, the CAAP aims to drive digital security awareness and readiness to the wider business community in Singapore. This virtual event in collaboration with the Personal Data Protection Commission (PDPC), hopes to promote Singapore organisations' understanding of incident response management in a mock data breach incident.

About the workshop

98 workshop participants have been pre-assigned to different departments for the tabletop exercise (TTX) based on simulated data breach for *a Singapore SME*, for this virtual workshop on 23 September 2020. This was conducted during the Privacy Awareness Week 2020 by the PDPC.

Seven facilitators have been assigned to assist in the participants' queries and guiding the participants from enterprises and SMEs throughout the exercise.

During a data breach, time is of essential.

Participants have to make quick decisions based on incomplete information and under time constraints. Thus, they should discuss with their team ('department') on the pros and cons for the decision made or information required by other departments, including the management. It is important to assess the risk in the collective decision-making and the justification.

Participants' demographics

Data Protection Officers (DPOs) and individuals holding middle to senior management-level positions that focus on:

- Develop policies and strategies to manage their organisations' data activities and cybersecurity posture and compliance to legal, industry and customer requirements.
- Implement policies and processes, and possibly to develop the processes to support the organisations' policies.
- Ensure organisations' resources, capabilities and capacity in handling incident response and data breaches, with some oversight on personnel's competencies in this aspect.
- It is not necessary for the participants to have technical background in information or cyber security or be trained in PDPA or GDPR to attend the TTX.

Our participants hold middle to senior management roles in various departments, such as administration, human resources, marketing, operations, IT and legal.

The intended outcomes for the participants are as follows:

- Understand the general principles and be equipped with the knowledge of incident response management in the context of Singapore's PDPA.
- Understand how the various stakeholders including external parties, can support or derail organisation's efforts to manage data breaches.
- Understand the steps all personnel within an organisation can follow and to support a corporate culture of responsible and accountable usage of personal data.

At the point of publication, the Singapore Parliament has passed changes to the Personal Data Protection Act on 2 Nov 2020, including stiffer penalties for data breaches. We hope our simple scenario contextualised for a Singapore SME's context can help companies to start planning their data breach responses.

TTX Scenario

Participants are working in a Singapore-based manufacturing company with overseas suppliers and B2C customers. The company has implemented work-from-home arrangement hastily during COVID-19 pandemic.

The company experienced a data breach when one of the colleagues clicked on a phishing email. This led to disclosure of sensitive personal data of the company's customers and staff, and the company's VPN was compromised.

In this SME, there are several departments that need to coordinate resources and responses as part of its incident management response, participants are in one of the following departments,

1. Management
2. Finance
3. Administration/ HR
4. IT
5. Corporate Communications or PR, including crisis communications
6. Sales and marketing, business development
7. Operations, logistics, supplier management

Participants are asked to think through the incident response their departments need to give. For instance, Comms Department has to prepare a statement for media queries and customers.

Incident Response Management

What is Incident Response Management (IRM)?

Incident response is all about planning ahead and having a plan before it is necessary to activate it. Managing incident response includes testing your plan, with specific business outcomes in mind, and update your plan when conditions change.

Why must companies have IRM in place?

Any incident that is not properly contained and handled can escalate into a bigger problem that can further lead to a damaging data breach, large expense or system collapse.

Responding to an incident quickly will help an organisation minimise losses, mitigate exploited vulnerabilities, restore services and processes and reduce the risks that future incidents pose. For instance, the SingHealth data breach may have turned out differently if its incident response management was robust. Please refer to our Annex section on our summary based on PDPC's decision.

Who should be involved in IRM?

Depending on the organisational structure,

1. Board of Directors
2. Management
3. Finance
4. Administration
5. HR
6. Operations
7. IT
8. Procurement
9. Business Continuity Management/Compliance/Legal/Risk Management
10. Customer Service
11. Corporate Communications or PR, including crisis communications
12. Sales and marketing
13. Suppliers for manufacturing materials
14. External IT vendors

For large organisations, incident response activities are usually conducted by the organisation's computer security incident response team.

Incident Response Management

What are the key components of IRM?

The incident response team follows the organisation's IRP, which is a set of written instructions that outline the organisation's response to incidents and confirmed breaches. IRP refers to Incident Response Plan.

Plan – you have to first plan out how your company would respond during an incident.

Test – A plan is only good on paper if your company does not test to verify that it works. Companies can test out their plan during tabletop exercise but it is common to see SMEs only manage to use their plans for the first time in an actual incident or data breach.

Update – The plan needs to be updated to make sure it works realistically during an actual incident. Companies can update their plan after each exercise, or when there is change in the business directions e.g. having a new third-party vendor that processes your personal data, change in regulations, or after a data breach.

According to the SANS Institute, there are six key phases of an incident response plan:

- *Preparation*: Preparing users and IT staff to handle potential incidents should they should arise.
- *Identification*: Determining whether an event qualifies as a security incident.
- Containment: Limiting the damage of the incident and isolating affected systems to prevent further damage.
- *Eradication*: Finding the root cause of the incident and removing affected systems from the production environment.
- *Recovery*: Permitting affected systems back into the production environment and ensuring no threat remains.
- *Lessons learned*: Completing incident documentation, performing analysis to learn from the incident and potentially improving future response efforts.

Incident Response Management

When you should test your IRM?

A plan is only good on paper if your company does not test to verify that it works. Besides testing your IRM and the effectiveness you are measuring it on after your first plan is out, your IRM should ideally be tested when,

- There are updates in the IRP.
- Your company has a new third-party vendor that processes your personal data.
- There are changes in regulations.
- New client asked for proof on your company's IRM and data breach protocol and procedures.
- New colleagues are to be trained in handling incidents in their respective areas of work.

How do you develop IRM capabilities?

Companies' IRM capabilities should support the business outcomes, desired responses to stakeholders including media, and at the basic level, proper, realistic and effective execution of the IRP.

For instance, if one key risk from inadequate incident handling is negative media reporting, then the organisation needs to have crisis communications in place where the spokesperson needs to be trained to handle media under stress. There should also be proper communication policies and SOPs so that staff are aware not to speak to media or make social media posts.

Risk Management

Companies should conduct proper risk assessment whether to notify individuals affected by the personal data breach, and if they should notify the PDPC as well. This requires objective justification, proper discussion based on accurate information and rigour in the informed decision-making process.

It is important to weigh the implications involved holistically if one choose to notify or not to notify. Companies need to be clear if there is significant harm to the individuals or is of a significant scale. They will also be required to notify affected individuals if the data breach is likely to result in significant harm to the latter.

During the workshop in September 2020, we covered that companies should conduct proper risk assessment whether to notify individuals affected by the personal data breach, and if they should notify PDPC as well. This is a demonstration of the companies' accountability.

The Personal Data Protection (Amendment) Bill 2020 was passed on 2 November 2020. Some areas of interest to companies pertaining to risk assessment are as follows:

1. To further strengthen organisations' accountability, Clause 13 introduces a system for mandatory notification to the PDPC when a data breach occurs.

    - In addition, organisations must notify both the PDPC and affected individuals when data breaches result, or are likely to result, in significant harm to individuals. Organisations have the duty to conduct assessment of data breaches with regard to the scale and impact of data breaches.

    - This is also extended to a data intermediary of a public agency.

2. Clause 7 introduces the new section 15A, which expands the consent regime by introducing deemed consent by notification. Under this provision, organisations may notify their customers of the new purpose and provide a reasonable period for them to opt out.

    - Before doing so, organisations must conduct a risk assessment and conclude that the collection, use or disclosure of personal data in this manner will not likely have an adverse effect on the individual.

TTX Simulation

First injection

IT department reported that a colleague from Operations department has clicked on a phishing email sent by an overseas supplier.

Operations has checked with the sender of the phishing email; it is not the supplier the company knows. Someone has impersonated the supplier and conducted a social engineering incident on the colleague. The link in the phishing email led to a malware downloaded to the colleague's laptop. The malware has enabled the attacker to alter the VPN settings where anyone can access and retrieve the confidential information without password.

Participants then discussed on what their departments would do in the context of the specified department's roles and responsibilities.

Second injection

Operations department reported that the colleague who clicked the phishing email, shared the sender knows how long the colleague has been working in the company and the names of his supervisor and other Operations, HR and Finance colleagues.

The shared folders containing company's financial reports, suppliers' contracts, personal data of customers and staff, and staff's curricula vitae, and health records of 50 staff are accessible in the 'open' VPN.

The company has around 5,000 B2C customers and their purchases are delivered to their residential addresses in Singapore and overseas. It also serve around 500 large B2B customers. B2C refers to business-to-consumer while B2B refers to business-to-business.

TTX Simulation

Second injection

Participants then discuss on their departments' recommended incident responses, as well as the type of input, information and approval needed from other departments. Six departments shared the following:

Recommended Responses	Input / Information Needed	Approval required
Administration/ HR		
1. Committee meeting and document all steps and discussion 2. Contain the damage Liaise with IT on this e.g. isolating the network/ system of affected personnel. 3. Assess the damage/ impact. How many affected individual and customers? B2B customers - if it involves as well Personal data. 4. Determine if to inform the individuals and PDPC. Committee to decide on this. PR to handle communication (both internal and external) especially to external parties. 5. Evaluate the situation and how to prevent such things from happening again. Training for future prevention.	1. IT - on damage/ impact assessment, root cause, prevention 2. PR - communication draft / statement 3. Compliance/ risk/ legal - if there is any legal impact	DPO to advise to committee after findings MD office - final decision to go ahead

TTX Simulation

Recommended Responses	Input / Information Needed	Approval required
Finance		
1. Escalation to IT. 2. Breach can allow financial records of the company to be compromised. 3. Financial records / payment details of customers. 4. What is the culture of the company? (Whistle-blow or report to authority) 5. Regulatory penalties. 6. Fines by PDPC i. Alert to CFO ii. Overseas customers (if in EU then GDPR imposes a 4% fine, queries from GDPR commission) 7. Fees incurred to: i. External auditors ii. Lawyers iii. Communication media agencies 8. Table a paper to the Board on the financial impact of such a breach on the company 9. One way for finance to mitigate the risk is through cybersecurity insurance to insure SMEs (products available in the market already). i. Coverage is on residual risk and insurer would do due diligence on whether SME has cybersecurity protections in place. 10. Suppliers' contracts would have confidentiality provisions so damages payable. 11. Bank accounts – approval for payments to be tracked / scrutinised payments. 12. Good cyber hygiene practices need to be in place.	Information required from IT and management (as in earlier point)	Approval required from management

TTX Simulation

Recommended Responses	Input / Information Needed	Approval required
IT		
1. Containment and stop the breach (VPN, pull logs). 2. Ring fence potentially affected systems (CRM, HR, Medical Claims, SAP)	1. Logs from system. 2. Pull email records and source of attack (URL & IP address). 3. Ask departments to review exfiltrated data for impact to consumers and vendors.	Senior management approval to shut down VPN due to business impact and explore alternative working arrangements (WFO, social distancing) due to COVID19 WFH requirements.
Management		
1. Ask respective departments to identify individuals whose personal data (particularly, sensitive personal data). 2. Manage communications (damage control) with regulators (PDPC) and customers/clients. Consider whether external professional help might be required to support this.	1. HR to identify employees/staff who are affected. 2. Ops and BD teams to identify key customers/clients to be approached proactively with relevant communication. Smaller customers/clients can perhaps be dealt with by 3. Finance to check our accounts and make sure that nothing affecting our financials. 4. IT to see whether we can disconnect affected systems without adverse implications (and also isolate and try to remedy the breach). 5. Compliance/Legal to see whether other data protections laws in other countries might impose obligations on us also (and not just the PDPA in Singapore).	Management's role is to act as a central hub of control and decision-making.

TTX Simulation

Recommended Responses	Input / Information Needed	Approval required
Operations, logistics, supplier management		
1. What is the input required from IT to facilitate this investigation? 2. Who is the coordinator? 3. Establish who clicked the email? 4. Check with supplier if there is data breach at their end? 5. Is there data sharing arrangement with this supplier? 6. To establish if the email was sent to anyone else?	See 1, 2, and 6 under *Recommended Responses*	No
Sales and marketing, business development		
1. Assemble a Crisis Management Team 2. Adopt the CARE approach	1. Need a script from Comms department, which should be a consistent and positive message. 2. Need drawer statements, FAQs to corporate clients and other customers. 3. Who is the DPO?	Need management decision on what and when to send to corporate clients and other customers.

TTX Simulation

Tasks for departments

All departments are tasked to complete key tasks quickly as part of the company's responses to the personal data breach.

TASKS AND DEADLINES FOR DEPARTMENTS			
Management 1) Decide if all B2C online transactions to be temporarily suspended. 2) Clarify Finance's budget before approval.	**Finance** 1) Submit contingency budget to Management for approval. 2) List out payment collection process for non-online orders.	**Admin/HR** 1) Make an official announcement to all staff on the data breach. 2) List out processes to monitor staff's social media posts in case of leakage.	**IT** 1) Update Management on remediation done. 2) Recommend to Management if VPN should be temporarily suspended.
Comms 1) Prepare statement for media queries, customers, business partners and regulators.	**Sales & Marketing** 1) Recommend to Management whether to inform customers on the data breach.	**Operations** 1) List out processes for non-online orders for customers.	

To notify or not to notify

The company has to decide whether to notify or not notify PDPC on the personal data breach, it has to consider whether to inform individuals (customers, staff) affected as well. All departments must agree on the collective decision whether their company should notify PDPC on the data breach.

After sharing their recommendations, all departments agreed that the company should inform the Commission.

Observations

The participants have been assigned to departments they are familiar with and not necessarily based on their current job roles, due to the sign-up rate and actual turnout at the workshop. We would also like the participants to experience how their colleagues from other departments have to cope during a personal data breach. Importantly, no department nor personnel would be excluded from helping the organisation to tide through a crisis.

Facilitators' broad observations are as follows,

- Most participants are able to give practical input throughout the exercise and some leveraged the insights of other participants during the discussions.

- Some departments know who or which department they can request for information, but not many are keenly aware of what they need to do as data protection officers (DPOs).

- Some participants do not appear to be cross trained as DPOs even though they are part of the committee within their respective organisations.

- Some participants do not demonstrate adequately if they are ready to handle the incident on their own.

Recommendations

In light of the mandatory data breach notification (November 2020) under the PDPA Clause 13, we have some recommendations for our participants and companies with plans to enhance their incident response plans,

1. The DPO role should be clearly articulated and consistently applied within the organisation. DPO is not the only one responsible for IRM and addressing the personal data breach; it is a collective responsibility.

2. Organisation should list out their guidelines and course of action during an incident. Key decision makers are identified ahead so that they know what information they need beforehand.

3. There should be an owner for the escalation at the various levels, such as Head of Departments, DPO, Chief Information Security Officer and Management. The escalation chain should include the leadership involved, for accountability.

4. As the PDPC's broad-based guide is meant to cater to the needs of most companies in Singapore, it is important for companies to internalise the key points, plan out and then test their plans based on the identified risks.

5. We strongly encourage companies to test their incident response plan once a year as market conditions, technological updates and regulations may change from time to time. It is important for your plan to be realistic and implementable. Remember **plan**, **test** and **update**!

AiSP has received good responses from the participants and noted the limitation with the virtual TTX. We hope to hear from our participants if they have any suggestion for future TTX workshops. Please click **here** to submit by 31 March 2021.

Annex - Reflecting on IRM in the SingHealth Data Breach

Excerpt from PDPC's enforcement decision

Based on forensic investigations by IHiS and CSA, the attacker gained initial access to the SCM network in August 2017 by infecting a user's workstation. This was likely through an email phishing attack, which led to malware and hacking tools subsequently being installed and executed on the user's workstation. The attacker was able to gain access to an unpatched end-user workstation running a version of Outlook by using a publicly available hacking tool.

An IHiS database administrator realised the failed attempts to log in were evidence of someone attempting to gain unauthorised access to the database. On 13 June 2018, staff members from the IHiS Delivery Group met with the Security Management Department (SMD) over these login attempts. A chat group was created; members included the Security Incident Response Manager (SIRM), the SingHealth CISO and members of SMD.

13 days later, the attacker managed to obtain login credentials for the SCM database from the H-Cloud Citrix server. To compound matters, IHiS updated the SingHealth CISO that the software firewall rules had been implemented without having verified this. Vulnerabilities that had previously been flagged out to IHiS during audit were either not remediated or not addressed in time.

Between 27 June and 4 July 2018, the attacker used the stolen SCM database login credentials to access and run numerous bulk queries from one of the compromised SGH Citrix Servers on the SCM database. The staff of the IHiS Delivery Group who were not members of the SMD, alerted the Security Incident Response Team (SIRT) which is part of the SMD, and SIRM.

The SIRT was not formally activated at any point, which was not in accordance with IHiS' Healthcare IT Security Incident Response Framework and Cluster IT Security Incident Response SOP.

The SIRM and the SingHealth CISO were both aware of the suspicion of attack since 13 June 2018 and the remediation efforts of 4 July 2018. The CISO did not make further enquiries, he waited passively for updates instead. for updates. The SIRM was overseas until 18 June 2018 without nominating a covering officer. Neither the SIRM nor the SingHealth CISO escalated the matter despite their knowledge of these circumstances.

IHiS senior management and the SingHealth Group Chief Information Officer (GCIO) were only alerted to the attack on 9 July 2018. SingHealth GCIO promptly escalated the matter and informed the CEO of suspected unauthorised access into the SCM database.

Concurrently, the SingHealth GCIO informed the SingHealth Deputy Group Chief Executive Officer (Organisational Transformation and Informatics) (DGCEO (OT&I)).

Annex - Reflecting on IRM in the SingHealth Data Breach

Details of the attack and the exfiltration of data were first shared with the IHIS CEO and the SingHealth GCIO, on 10 July 2018. A "war room" with five working cells for containment, investigation, patient impact, communications and reviewing of security measures for other systems was also set up. From 10 July 2018, IHiS and CSA worked jointly to put in place containment measures to isolate the immediate threat, eliminate the attacker's foothold and prevent the attack from recurring.

On 19 July 2018, attempts by the attacker to access the SCM network were again detected and Internet Surfing Separation ("ISS") was instituted immediately thereafter on 20 July 2018 for SingHealth.

Shortly after SingHealth was informed of the cyber attack, SingHealth made plans for patient communications using multiple channels of communication. Within days after the public announcement of the cyber attack on 20 July 2018, SingHealth notified patients whether their data was illegally accessed and how they can seek help. Telephone hotlines were also set up for members of the public to obtain further information. Public could also check whether their data had been accessed on the "HealthBuddy" mobile application and the SingHealth website. On 1 November 2018, IHiS announced that it will be adopting a slew of measures to strengthen cybersecurity across the public healthcare sector following the cyber attack.

The illegal access and copying was limited to a portion of the SCM database, including:

a) the names, NRIC numbers, addresses, gender, race, and dates of birth ("Patient Particulars") of 1,495,364 SingHealth patients; and
b) the outpatient dispensed medication records of 159,000 patients (which is a subset of the full set of illegally accessed personal data).

SingHealth CISO is charged with security oversight for SingHealth and reports to the SingHealth GCIO directly on security matters.

The SingHealth CISO does not have any staff reporting under him and relies on the IHiS Delivery Group (specifically the SMD) for their technical expertise on security and operational matters.

The SingHealth CISO has a key role in the organisational structure of SingHealth with regard to IT security.

SingHealth CISO's failure to comply with various incident response policies and SOPs, IT security incident reporting processes and failure to exercise independent judgement did not demonstrate SingHealth had taken reasonable and appropriate measures to prevent unauthorised access and copying from the SCM database. It also point to a **larger systemic issue** within the organisation.

Annex - Reflecting on IRM in the SingHealth Data Breach

It also point to a **larger systemic issue** within the organisation.

The CISO did not escalate these security events but wholly deferred to the SIRM's assessment as to whether an incident was reportable (who operated under the misapprehension that a cyber security incident should only be escalated when it is "confirmed") when he should have exercised independent judgement to escalate the incident to the SingHealth GCIO. To his mind, at the time that he was informed of these suspicious activities, they were only potential breaches and were not confirmed security incidents as investigations were still underway. This does not comply with the IR-SOP.

The Public COI Report also highlighted that even within the IHiS SMD, the processes for reporting observations were inconsistent and unclear. There was no established procedure for how IHiS staff should escalate a matter internally or how to report a security incident to the SingHealth CISO or the SingHealth GCIO. This resulted in confusion and consequent delays in response. The COI also found at that SMD had delayed reporting because he felt that additional pressure would be put on him and his team once the situation became known to management.

As all IT functions and capabilities for the public healthcare sector, including the domain expertise and technical capabilities required to investigate and respond to IT security incidents, are centralised in IHiS, the SingHealth CISO and GCIO Office have to rely on the IHiS SMD for their oversight on cybersecurity incidents.

The SingHealth GCIO is supported by the GCIO Office, which has a staff strength of about 50 IHiS employees. Together, they are collectively responsible for 11 institutions, with an estimated 30,000 employees, 400-odd IT systems and 350 to 500 IT projects. The SingHealth CISO's responsibilities in the GCIO Office are also relatively broad.

Given the size and scale of SingHealth's IT systems and network and the large databases of sensitive medical personal data, it is reasonable to expect that considerable resources would have been devoted. However, the SingHealth CISO worked alone and had no staff reporting under him.

Annex - Reflecting on IRM in the SingHealth Data Breach

When the CISO was on medical leave between 20 June 2018 and 3 July 2018, the IHiS SIRM was to cover the SingHealth CISO's duties and provide guidance on the investigation. This revealed a systemic problem in the way the SingHealth GCIO Office is staffed. The SingHealth CISO did not have the resources or the technical and IT security expertise for him to properly fulfil his functions.

SingHealth CISO also failed to understand the significance of the information provided to him or to grasp the gravity of the events that were happening.

According to IHiS, it maintained a comprehensive IT security incident and response framework, which consists of three measures – prevention, detection and response, for all systems under its purview. IHiS had admitted that while the SIRF and IT-SPS were made available via IHiS' intranet, it had not developed any written policy on IT security incident reporting for its non-security staff and no training. IHiS non-security staff did not have a good understanding of the importance and requirements for reporting IT security incidents.

SingHealth cyberattack: What you need to know

Excerpt from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---SingHealth-IHiS---150119.pdf

Reading Materials

1. Guide to Managing Data Breaches 2.0, PDPC
2. PDPC's Decision on SingHealth data breach (Singapore Health Services Pte. Ltd. & Ors.),
3. Incident Handler's Handbook - SANS Institute
4. Personal Data Protection Act 2012
5. Opening Speech by Mr S Iswaran, Minister for Communications and Information, at the Second Reading of the Personal Data Protection (Amendment) Bill 2020, 2 Nov 2020
6. Selected Contributed Contents by AiSP where companies can refer to, https://www.aisp.sg/publications.html

This white paper is made possible by our participants, volunteers, PDPC as well as our supportive partners. Thank you!

Our Volunteers from AiSP

Facilitators
Tony Low (lead facilitator)
Huynh Thien Tam
Adrian Oey
Catherine Lee
Freddy Tan
James Tan
Yvonne Wong (Supporting from secretariat)

Data and Privacy Special Interest Group Founding Members

Our Participants from various industries

Accommodation and Food Services
Administrative and Support Services
Aerospace and precision engineering
Arts, Entertainment and Recreation
Aviation
Business Development Solutions
Consulting
Education
Finance and Insurance
Fintech
Healthcare
Information and Communications
Manufacturing
Private Security Industry
Professional, Scientific and Technical
Real Estate
Recreational Club
Retail and Service
Ride hailing
Social Services
Technology
Technology - Software-as-a-Service
Technology and BPO
Trade, Associations and Chambers
Transportation and Storage (Logistics)
Travel & Tourism
Wholesale and Retail Trade

We hope to hear from our participants if they have any suggestion for future TTX workshops. Please click **here** to submit by **31 March 2021**.

This paper is published by AiSP Secretariat with input from volunteers.

AiSP

Advance Connect Excel

www.aisp.sg