Cyber and Data Breach Notification

Sanjeev Gathani

February 16, 2023

Watch the video and answer the questions

How did the breach happen?

Could have it been prevented?

What are the lessons learned from the incident?

Data Breach - Summary

What to do in the event of a Data Breach?

STEP 1

Containing the data breach to prevent further compromise of personal data.

STEP 2

Assessing the data breach by gathering the facts and evaluating the risks, including the harm to affected individuals. Where assessed to be necessary, continuing efforts should be made to prevent further harm even as the organisation proceeds to implement full remedial action.

STEP 3

Reporting the data breach to the PDPC and/or affected individuals, if necessary.

STEP 4

Evaluating the organisation's response to the data breach incident and consider the actions which can be taken to prevent future data breaches. Remediation efforts may continue to take place at this stage.

Aggravating Factors

- **The organization failed to actively resolve the matter** with the individual in an effective and prompt manner
- **Intentional, repeated and/or ongoing breaches** of the Data Protection Provisions by an organization
- **Obstructing the Regulator during investigations** (such as making efforts to withhold or conceal information requested by the Regulator)
- **Failing to comply with a previous warning or direction** from the Regulators
- **The organization is in the business of handling personal data** (such as medical or financial data), but failed to put in place adequate safeguards proportional to the harm that might be caused by disclosure of that personal data

- *Source: PDPC Singapore*

Mitigating Factors

The organization has actively and promptly tried to **resolve the matter with the individual**

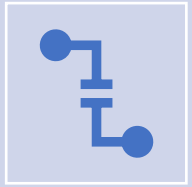
The organization has taken reasonable steps to prevent or reduce the harm of a breach (such as putting in place strong passwords and/or encrypting the personal data to prevent unauthorized access)

The individual affected by the breach has already received a remedy in some other form (for example, through a civil action against the organization)

Source: PDPC - Singapore

Mitigating Factors

The organization took immediate steps to reduce the damage caused by a breach (such as informing individuals of steps they can take to mitigate risk)



The organization voluntarily disclosed the personal data breach to the PDPC as soon as it learned of the breach, and co-operated with the PDPC in its investigations

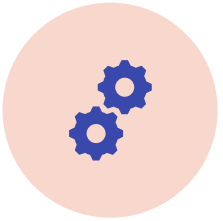
Source: PDPC - Singapore

Summary – Cyber and Data Breach Management

KNOW THE LAW

CREATE A DATA POLICY

CREATE AN EQUIPMENT POLICY



AUTOMATE WHAT YOU CAN

TRAIN AND EDUCATE

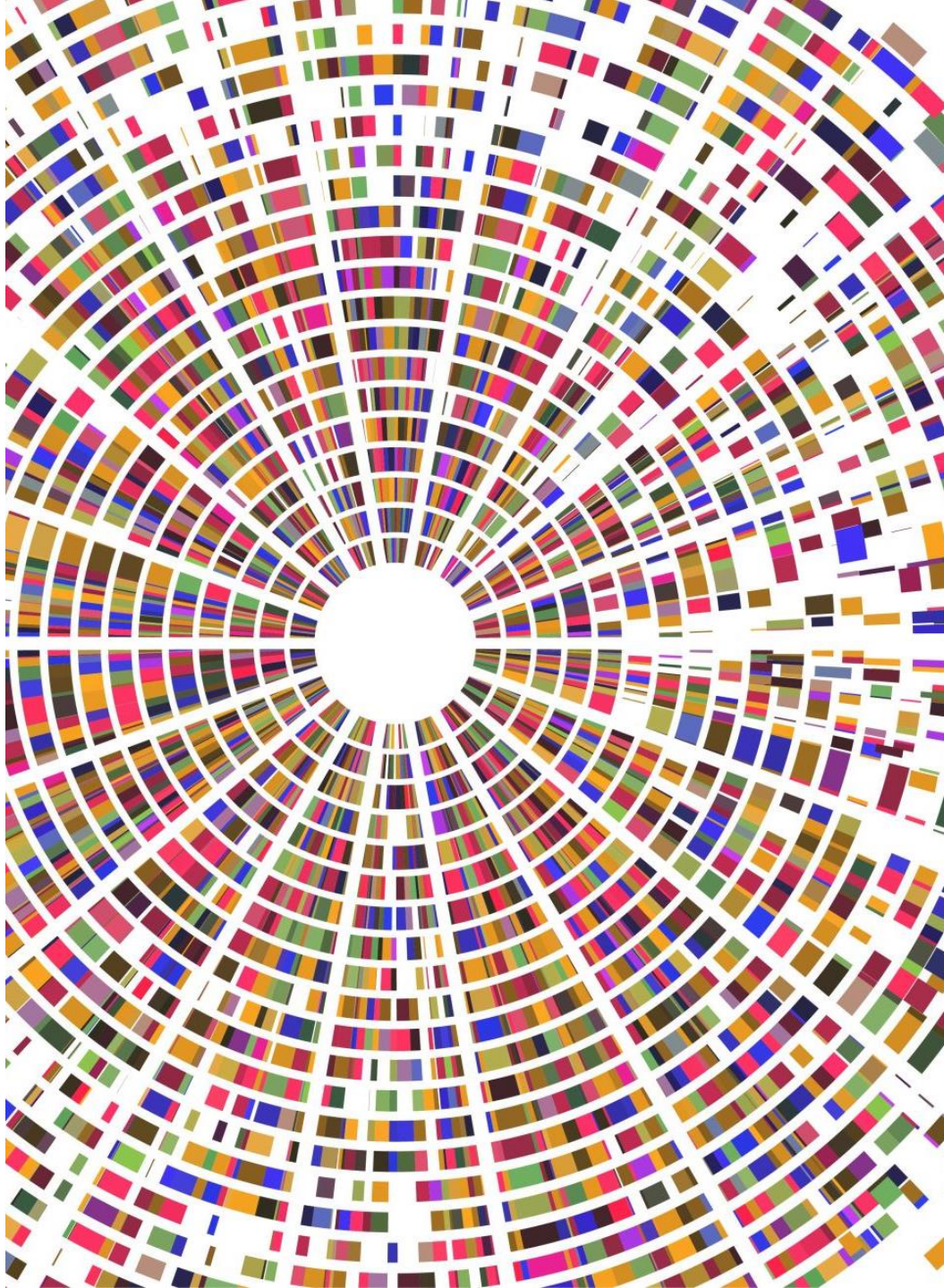
USE ENCRYPTION

Summary – Cyber and Data Breach Management

Use user authorization
Track and monitor usage
Practice patch management
Audit regular
Backup your data

Cyber and Data Breach Management

Obligations on the vendor or third party contractors to keep proper audit trails of its data and data security procedures, including in the event of data breach incident



FINAL SUMMARY – Cyber and Data Breach Management

Companies remain responsible for data breaches by their vendors, and not take a hands-off approach – Accountability cannot be outsourced

Maintain proper standards or lose customers trust

Obtaining indemnities

Proper audit trails of its data processing and data security procedures, including in the event of data breach incident

THANK YOU AND QUESTIONS