Plenary Session 3: Accountability, Legal Enforcement & Roadmap of the Data Privacy Law

Legal Enforcement / Accountability

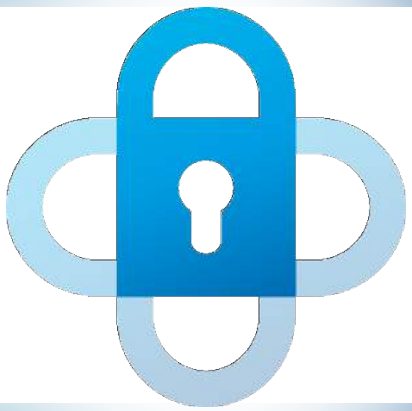
The CHAMBER Connects

Atty. Jeff E. Datingaling
CIPM (IAPP)


NATIONAL
PRIVACY
COMMISSION


LAST CALL BREACHES

Personal data breach



Security incident

NATIONAL PRIVACY COMMISSION

TYPES

Availability Breach

Due **to loss or accidental and unlawful destruction** of personal data

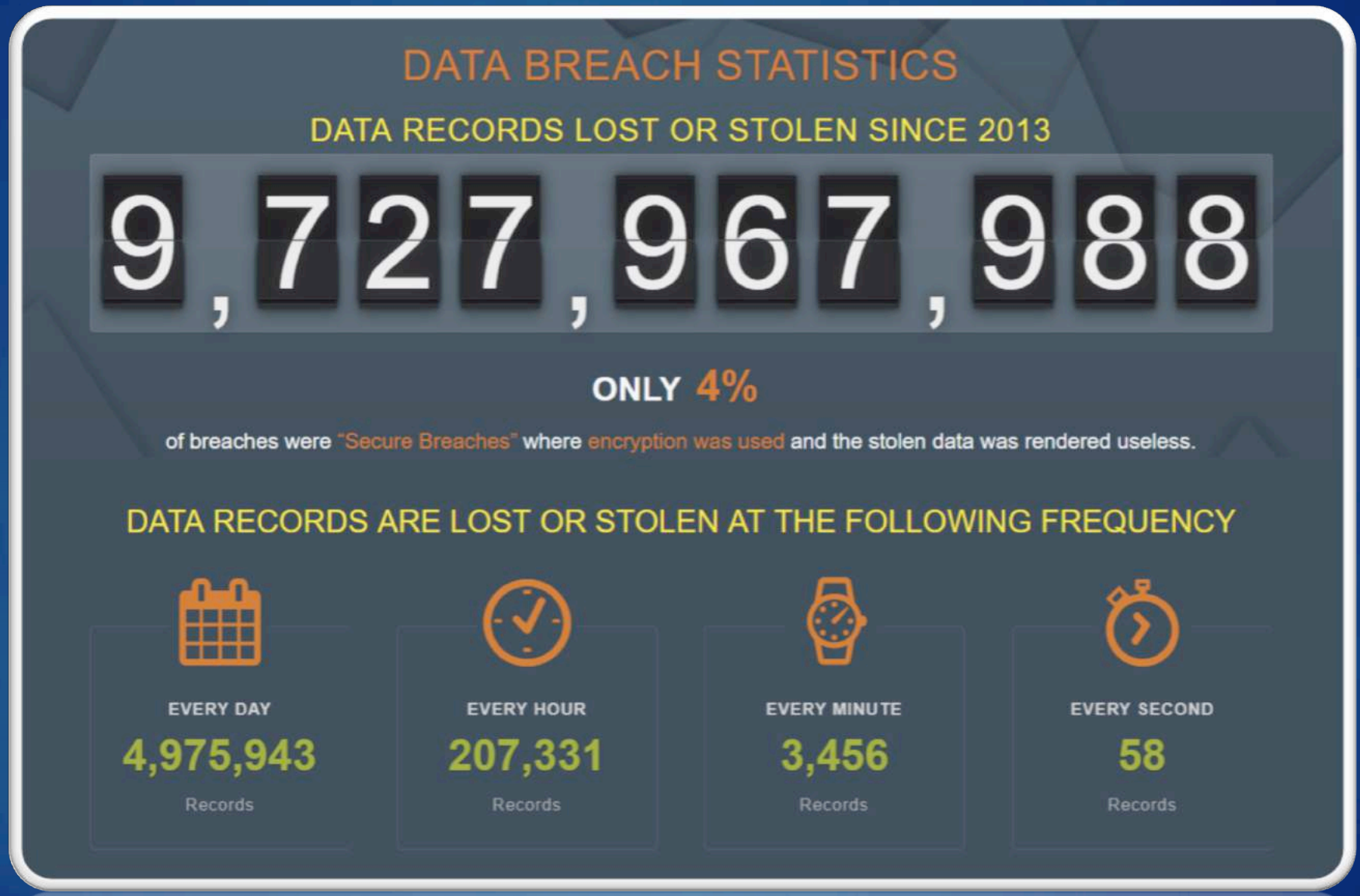
Integrity Breach

Due to **alteration** of personal data

Confidentiality Breach

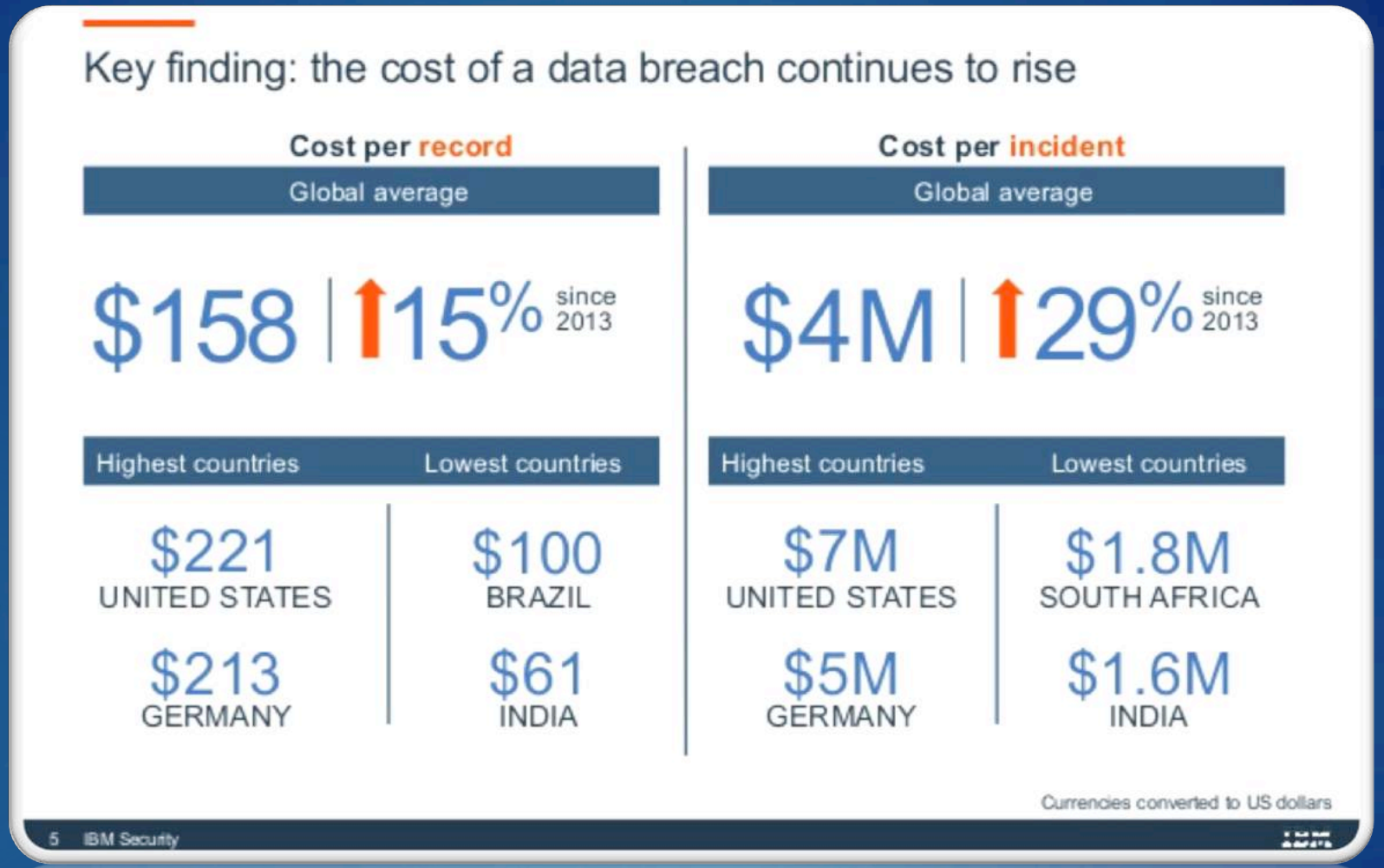
Due to **unauthorized disclosure of or access** to personal data

NATIONAL PRIVACY COMMISSION



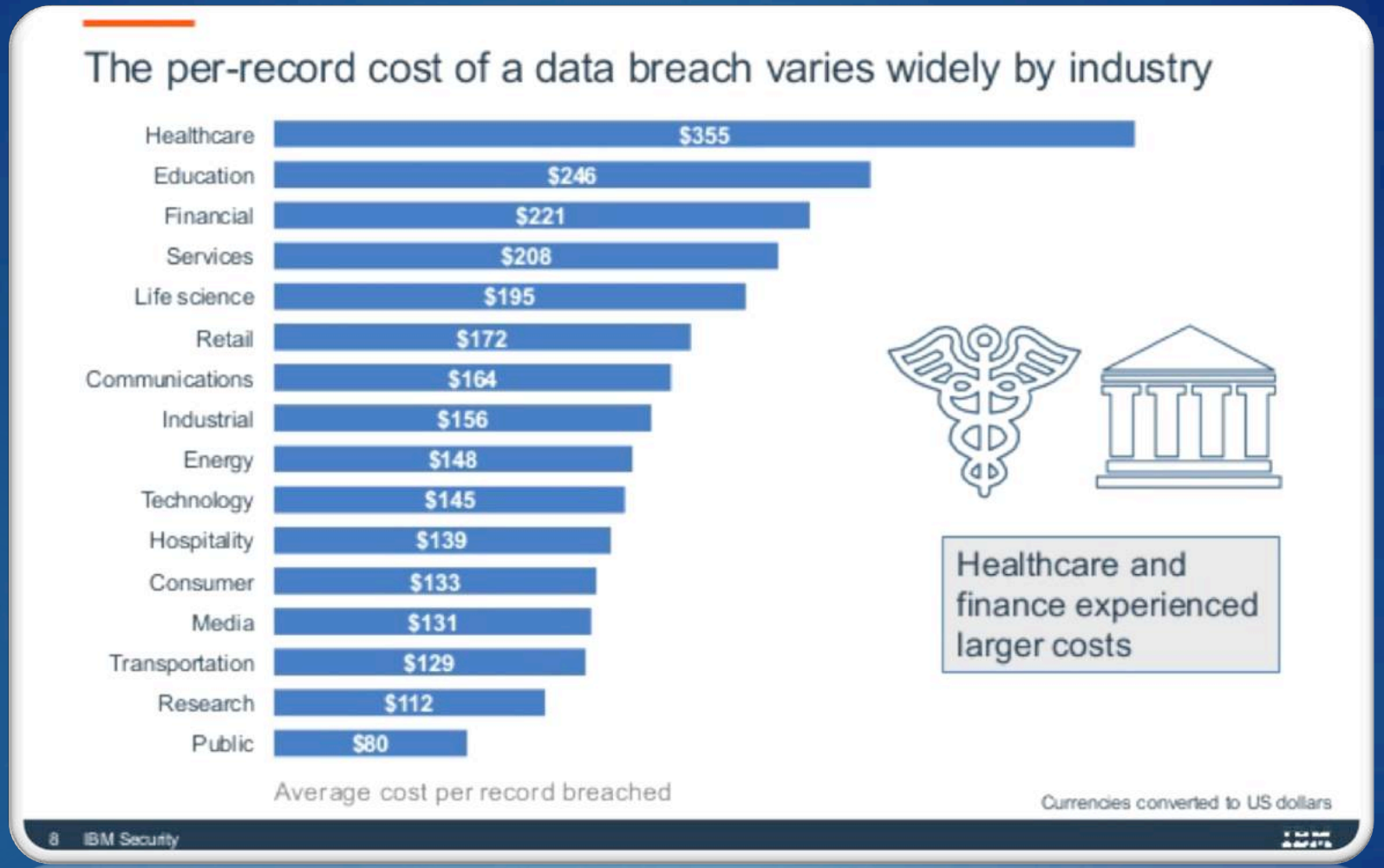
NATIONAL PRIVACY COMMISSION

Source: https://breachlevelindex.com/



Source: IBM Security
https://www.slideshare.net/ibmsecurity/the-2016-ponemon-cost-of-a-data-breach-study

NATIONAL PRIVACY COMMISSION



NATIONAL PRIVACY COMMISSION

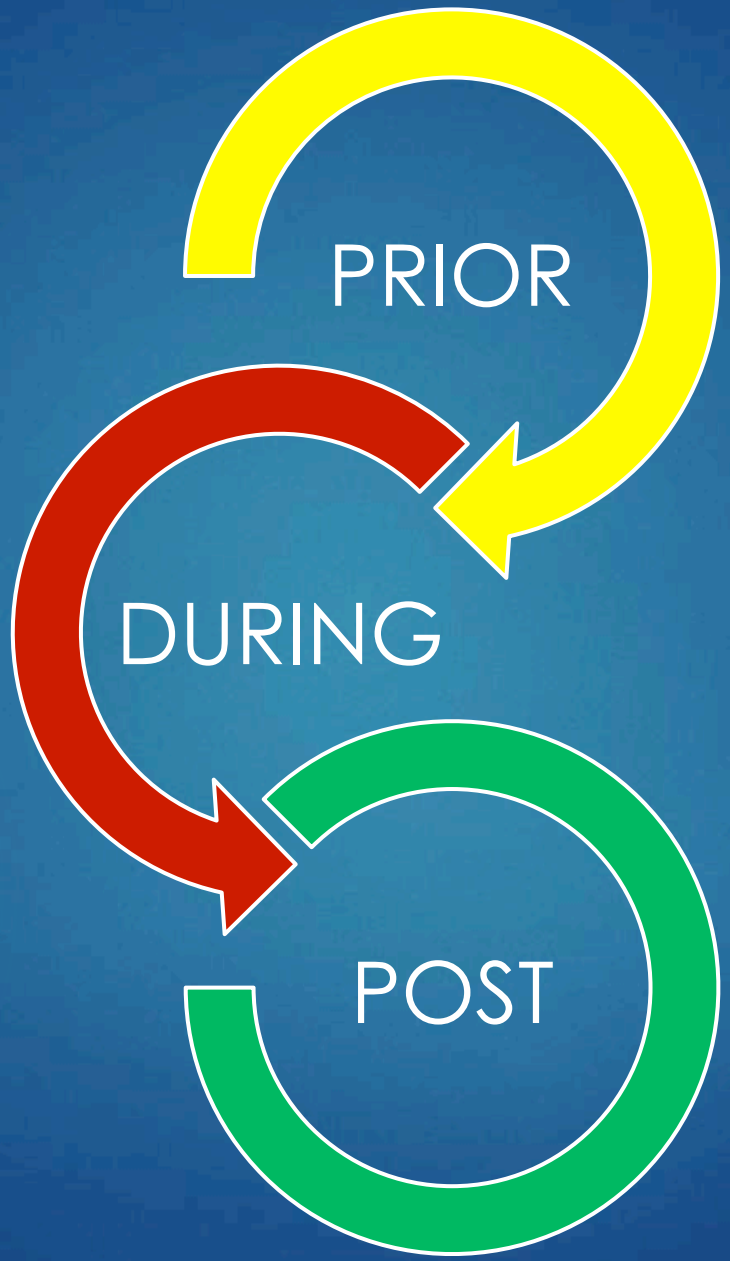
Source: IBM Security
https://www.slideshare.net/ibmsecurity/the-2016-ponemon-cost-of-a-data-breach-study

NATIONAL PRIVACY COMMISSION

Source: https://breachlevelindex.com/

Beauty and the Breach

HOW TO MANAGE BREACHES



NATIONAL PRIVACY COMMISSION

SECURITY INCIDENT MANAGEMENT POLICY

NATIONAL PRIVACY COMMISSION

https://goo.gl/images/XVdHBf

The data breach response team must have at least one member with the authority to make **immediate decisions on critical actions**.

The team shall be responsible for:

- Compliance with the security incident management policy
- Management of security incidents and personal data breaches
- Compliance with the data privacy law and other issuances

**This may be outsourced by the Personal Information Controller or Processor*

NATIONAL PRIVACY COMMISSION

PROTECT DATA SUBJECTS

NATIONAL PRIVACY COMMISSION

1. Conduct a **privacy impact assessment**
2. Have a working **data governance policy**
3. Implement **security measures**
4. Make sure personnel are **trained**
5. Regularly **review policies and procedures**
6. Be **aware** of threats

BEST PRACTICES

NATIONAL PRIVACY COMMISSION

https://goo.gl/images/fPRgK2

Breached?

NATIONAL
PRIVACY
COMMISSION

Notification of a data breach is **mandatory** when:

1. Data involves a. sensitive personal information or b. any other information that may be used to enable identity fraud.
2. There is reason to believe that the information may have been acquired by an unauthorized person; and
3. Gives rise to a real risk of serious harm to any affected data subject.

NATIONAL PRIVACY COMMISSION

WHO SHOULD NOTIFY?

The **Personal Information Controller** through the data breach response team.

Note: The obligation to notify remains with the Personal Information Controller even if the processing of information is outsourced or subcontracted to a Personal Information Processor.

NATIONAL PRIVACY COMMISSION

WHEN SHOULD NOTIFY?

The notification must be made within 72 hours upon knowledge of, or when there is reasonable belief that a personal data breach has occurred.

NATIONAL PRIVACY COMMISSION

WHO SHOULD BE NOTIFIED?

Notification must be made to the Commission and to any affected data subjects.

NATIONAL PRIVACY COMMISSION

HOW?

Notification to the Commission may be done through e-mail at complaints@privacy.gov.ph or through delivering a hard copy to the NPC office.

Upon receipt of the notification, the Commission shall send a confirmation message/e-mail to the Personal Information Controller.

A report is not deemed filed without confirmation.A read receipt report is not sufficient confirmation.

NATIONAL PRIVACY COMMISSION

HOW?

Notification may be made on the basis of available information within the 72-hour period if the personal data breach is likely to give rise to a real risk to the rights and freedoms of data subjects.

May be supplemented with additional information at a later stage on the basis of further investigation.

NATIONAL PRIVACY COMMISSION

HOW?

Notification to affected data subjects may be done electronically or in written form, but must be done individually.

The notification must not involve a further, unnecessary disclosure of personal data.

If individual notice takes disproportional effort, NPC authorization is required for alternative means.

NATIONAL PRIVACY COMMISSION

CONTENTS

- Nature of the Breach
  - Description of how the breach occurred and the vulnerability of the data processing system that allowed the breach
  - Chronology of the events leading up to the loss of control over the personal data
  - Approximate number of data subjects or records involved
  - Description or nature of the personal data breach
  - Description of the likely consequences of the personal data breach
  - Name and contact details of the data protection or compliance officer or any other accountable persons.

NATIONAL PRIVACY COMMISSION

CONTENTS

- Personal Data Possibly Involved
  - Description of sensitive personal information involved
  - Description of other information involved that may be used to enable identity fraud

NATIONAL PRIVACY COMMISSION

CONTENTS

- Remedial Measures to Address Breach
  - Description of the measures taken or proposed to be taken to address the breach
  - Actions being taken to secure or recover the personal data that were compromised
  - Actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident
  - Action being taken to inform the data subjects affected by the incident, or reasons for any delay in the notification
  - The measures being taken to prevent a recurrence of the incident.
  - Contact information or website containing information on how to mitigate damage arising from the data breach

NATIONAL PRIVACY COMMISSION

DELAY

Can’t make the 72-hour deadline?
Ask the NPC for an extension.

The NPC can also exempt you from data subject notification if notification is not in the public interest; or in the best interest of the data subjects.

NATIONAL PRIVACY COMMISSION

FULL REPORT

The full report of the personal data breach must be submitted within **five (5) days**, unless the Personal Information Controller is granted additional time by the Commission to comply.

NATIONAL PRIVACY COMMISSION

CONCEALMENT

An intention to conceal is presumed if the Commission does not receive notification from the personal information controller within five (5) days from knowledge of or upon a reasonable belief that a security breach occurred.

Concealment is a crime!

NATIONAL PRIVACY COMMISSION

SECURITY INCIDENT REPORT

NATIONAL PRIVACY COMMISSION

ANNUAL REPORT

DEADLINE: **JUNE 30, 2018**

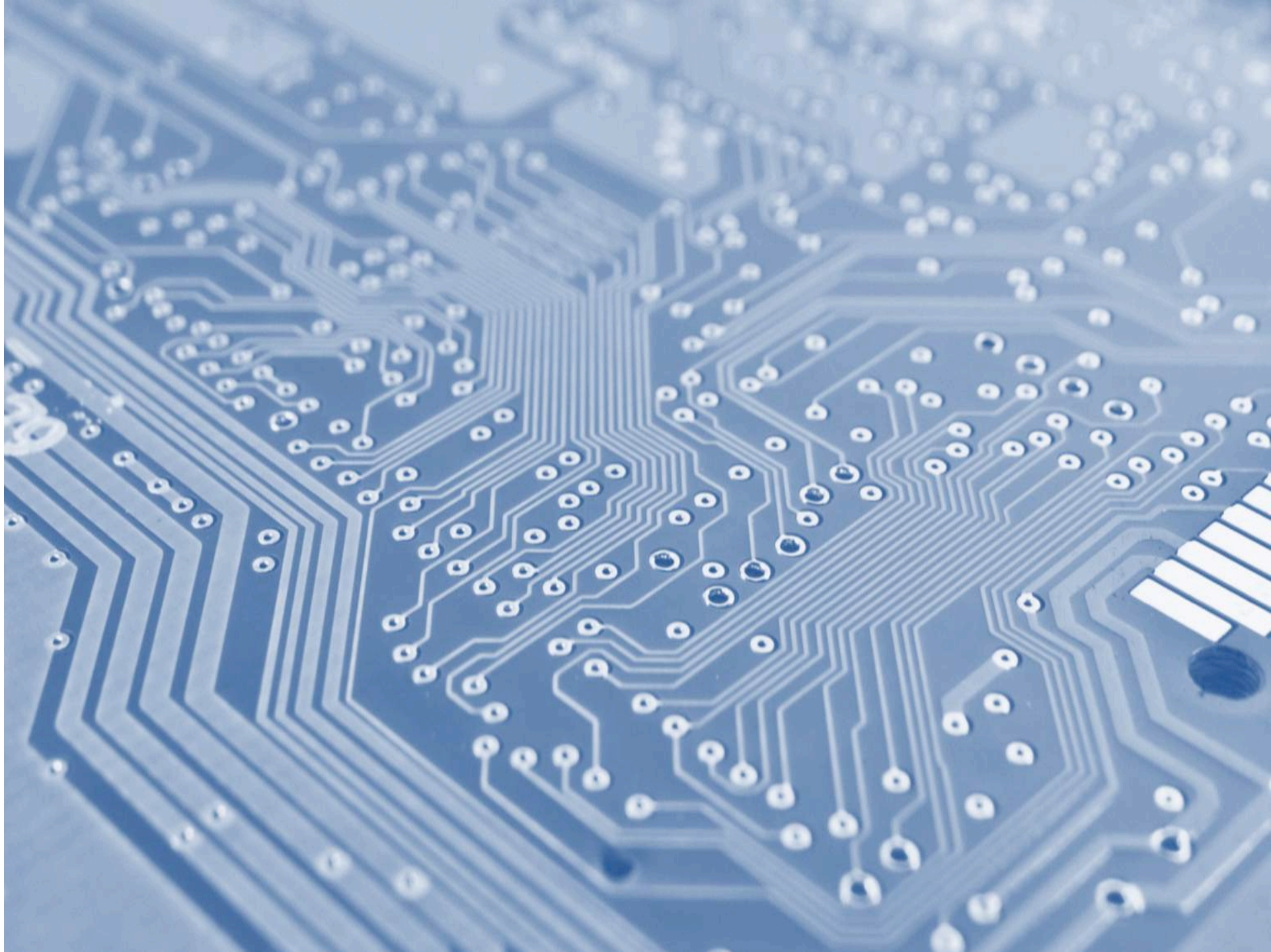
NOT AS COMPREHENSIVE AS A DATA BREACH NOTIFICATION

CONTAINS SECURITY INCIDENTS INCLUDING DATA BREACHES

DATA BREACHES MUST INCLUDE ALL REQUIRED INFOR UNDER THE NOTIFICATION REQUIREMENTS

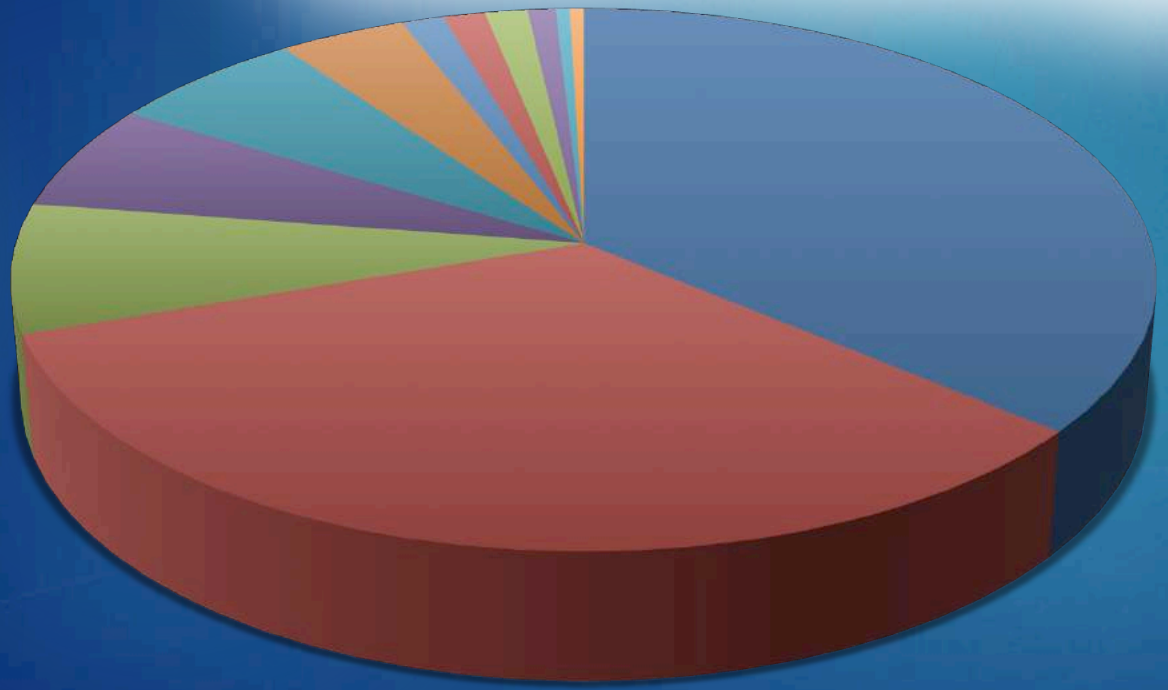
NATIONAL PRIVACY COMMISSION

ENFORCEMENT



NATIONAL PRIVACY COMMISSION

221 Complaints



NATIONAL PRIVACY COMMISSION

CRIMES

NATIONAL PRIVACY COMMISSION

CRIMES

7 years IMPRISONMENT
95,000 USD Max Fine
ADMINISTRATIVE FINES NOT YET INCLUDE

NATIONAL PRIVACY COMMISSION

FIRST CONVICTIO

NATIONAL
PRIVACY
COMMISSION

STOP PROCESSING ORDERS.

NATIONAL PRIVACY COMMISSION

Cross-border enforcement

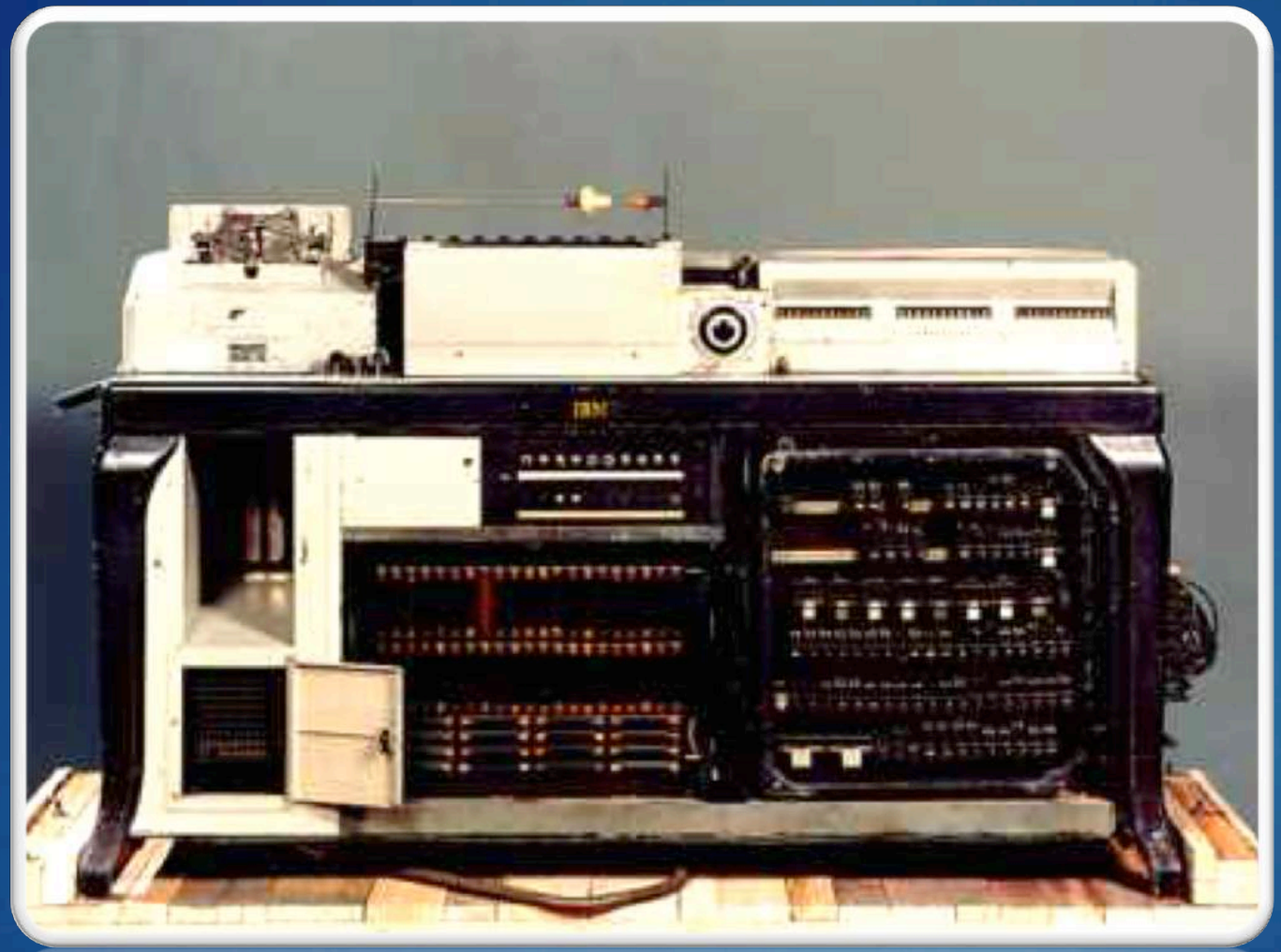
CPEA APEC Cross-B
Enforcemer

NATIONAL PRIVACY COMMISSION

REMINDERS

NATIONAL
PRIVACY
COMMISSION

NATIONAL
PRIVACY
COMMISSION



NATIONAL
PRIVACY
COMMISSION


NATIONAL
PRIVACY
COMMISSION
SAVING PRIVACY