BSBXCS402 Promote workplace cyber security awareness

Data protection and legislation

Data Protection

Data protection – the practices, safeguards and binding rules put in place to protect your personal information and ensure that you remain in control of it

Data Protection

You need to be able to :

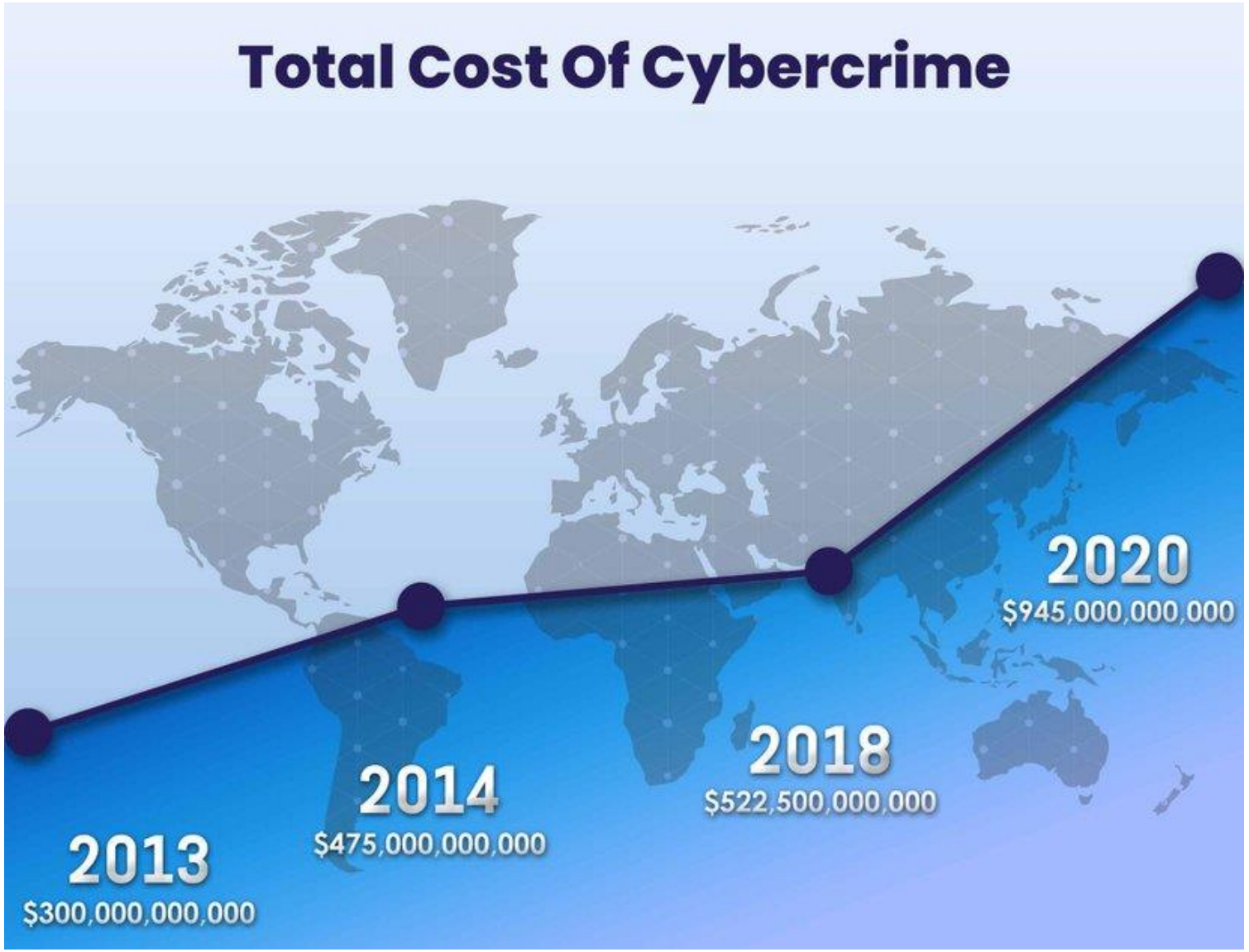
- Decide whether or not you want to share some information
- Who has access to that information
- For how long
- For what reason/use
- What can be modified

Data Protection

Governments have a vested interest, and play a role in protecting data.

- Cybercrime costs the global economy about 1 trillion — 50% more than that predicted in 2018. Also, it is more than 1% of the global GDP.
- The average cost of a data breach in 2020 was a whopping $3.86 million. In 2021 it was $4.24 million.
- A data breach compromising 1-10 million records costs $50 million on average, whereas one compromising 50 million records can cost as much as $392 million.
- 2021 Cyber Attack Statistics, Data, and Trends | Parachute (parachutetechs.com)

Data Protection

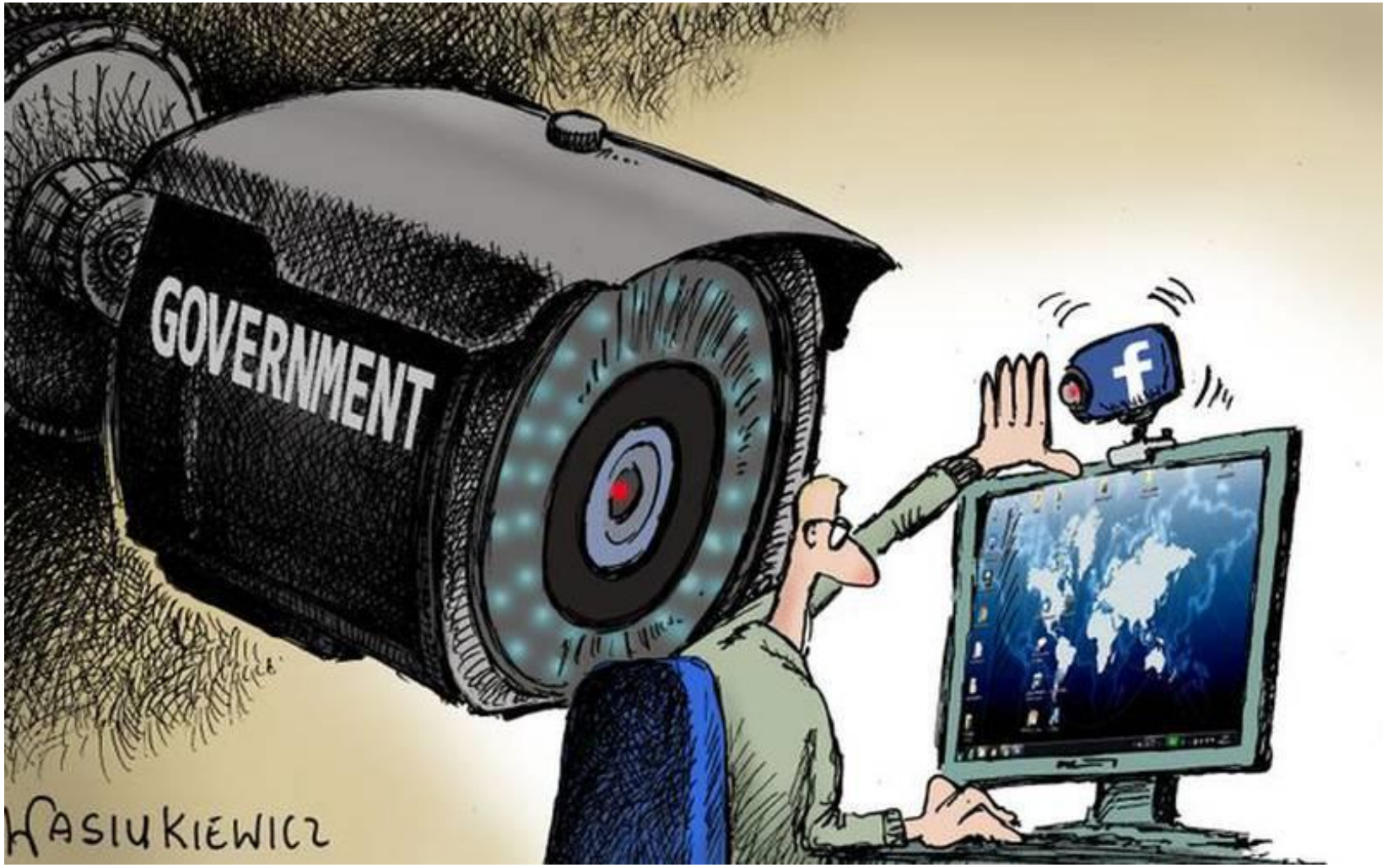


Data Protection Laws

There are 2 main reasons Governments are involved:

- Laws need to be updated to keep up with the changing world. Privacy laws exist in many countries to protect people's information and human rights, but they quickly go out of date in our rapidly changing connected world
- Many corporations have argued that flexible self-regulation mechanisms are the solution for protecting privacy and data. However these non-binding solutions have not achieved the desired results.

Data Protection Laws



Privacy Law

The Privacy Act 1988 : Section 14 defines the 13 Information Privacy Principles (IPPs)

These principles apply to government and non-government.

The principles define how and when data can be collected.

The law gives Australians the right to know why is information being collected about them, and who can see it.

The law makes those in charge of storing the information ensure that the data is neither lost or exploited.

Australian Privacy Principles

- An Open and Transparent Management of Personal Information
- Anonymity and Pseudonymity
- Collection of Solicited Personal Information
- Unsolicited Personal Information
- Notification of Collection of Personal Information
- Use or Disclosure of Personal Information
- Direct Marketing
- Cross-Border Disclosure of Personal Information
- Adoption, Use or Disclosure of Government Related Identifiers
- Quality of Personal Information
- Security of Personal Information
- Access to Personal Information
- Correction of Personal Information

NDB

The Notification of Data Breach Act (NDB) applies to any agency/organisation that is covered by the Privacy Act 1988

NDB

Under the Notifiable Data Breaches (NDB) scheme any organisation or agency the Privacy Act 1988 covers must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

The notification to individuals must include recommendations about the steps they should take in response to the data breach. You should notify the OAIC using our online Notifiable Data Breach form.

NDB

- A data breach occurs when personal information an organisation or agency holds is lost or subjected to unauthorised access or disclosure. :
- a device with a customer's personal information is lost or stolen
- a database with personal information is hacked
- personal information is mistakenly given to the wrong person
- The notification to individuals must include recommendations about the steps they should take in response to the data breach

Cybercrime Act

Computer and internal related offences such as unlawful access and impeding access to computer, computer related fraud, cyber stalking and child pornography. It is related to integrity of electronic communication and electronically stored data. It was amended on 1st march, 2013 and establishes framework for Australian access to council of Europe convention on cybercrime that works in collaboration with mutual assistance in criminal matters act 1987(Cth), Criminal Act 1914(Cth), criminal code and telecommunication Act 1979,offenses related to cybercrime bill 477.1 entitled to unauthorised access ,modification of restricted data, supply of restricted data held in credit cards and many forth.

Spam Act (2003)

Scheme for regulation of commercial emails and other type of electronic messages that restricts unauthorized messages with some exemptions. It is regulated by Australian communication and media authorities. Its fines non compliance firms up to 1.1 million dollars. (Acma.gov.au, 2018)Voice calls and fax messages are not covered by Australian media authority and managed by "do not call register. All messages should follow consent, identifiers and unsubscribe policies listed in this act·

Telecommunication Act (1997)

Primary objective is to protect privacy of individuals who use Australian telecommunication systems related to real time communications. It is amended to another law amended on 13 march,2015 through which(Alrc.gov.au, 2018) various agencies can access real time traffic after getting warrant from court .Metadata according to this law plays important role for national security agencies .Metadata includes telephone calls, websites access, geolocation details,. It works in collaboration with APP's.

Cyber terrorism conventions

ASIO responds to increased cyber threats that basically stand as advisor to improve national security by combating cyber terrorism with cyber security principles. This includes various laws: 1.Security Legislation Amendment (Terrorism) Act 2002 2.Suppression of the Financing of Terrorism Act 2002 (Cth) 3. Criminal Code Amendment (Suppression of Terrorist Bombings) Act 2002 (Cth). 4.Cybercrime bill 2012