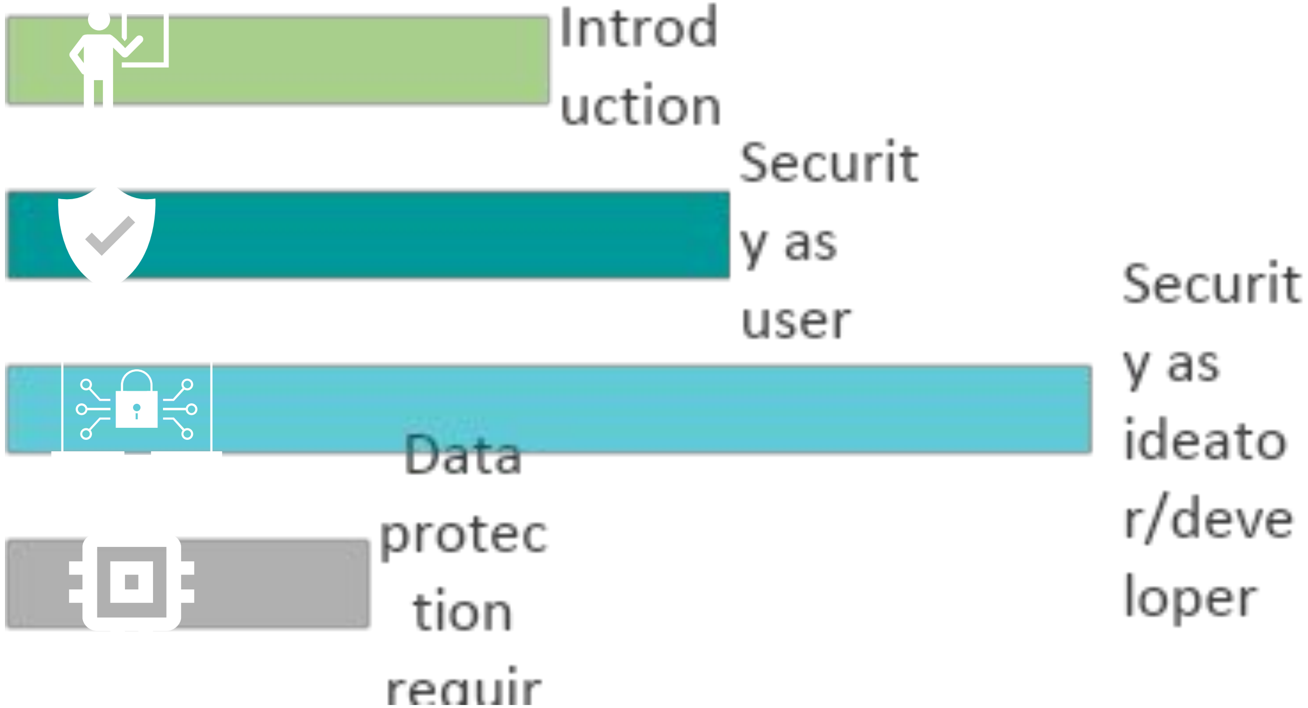
Open Source Software Security – Virtual Labs

Raakesh T
Principal Technical Officer
C-DAC, Ministry of Electronics and IT

In this session



Introduction

Security as user

Security as ideator/developer

Data protection requir

Which one to chose!

Proprietary

- They are copyrighted
- Since we pay, they are entitled to fix as and when they occur bug is found.
- Continued support until sunset.

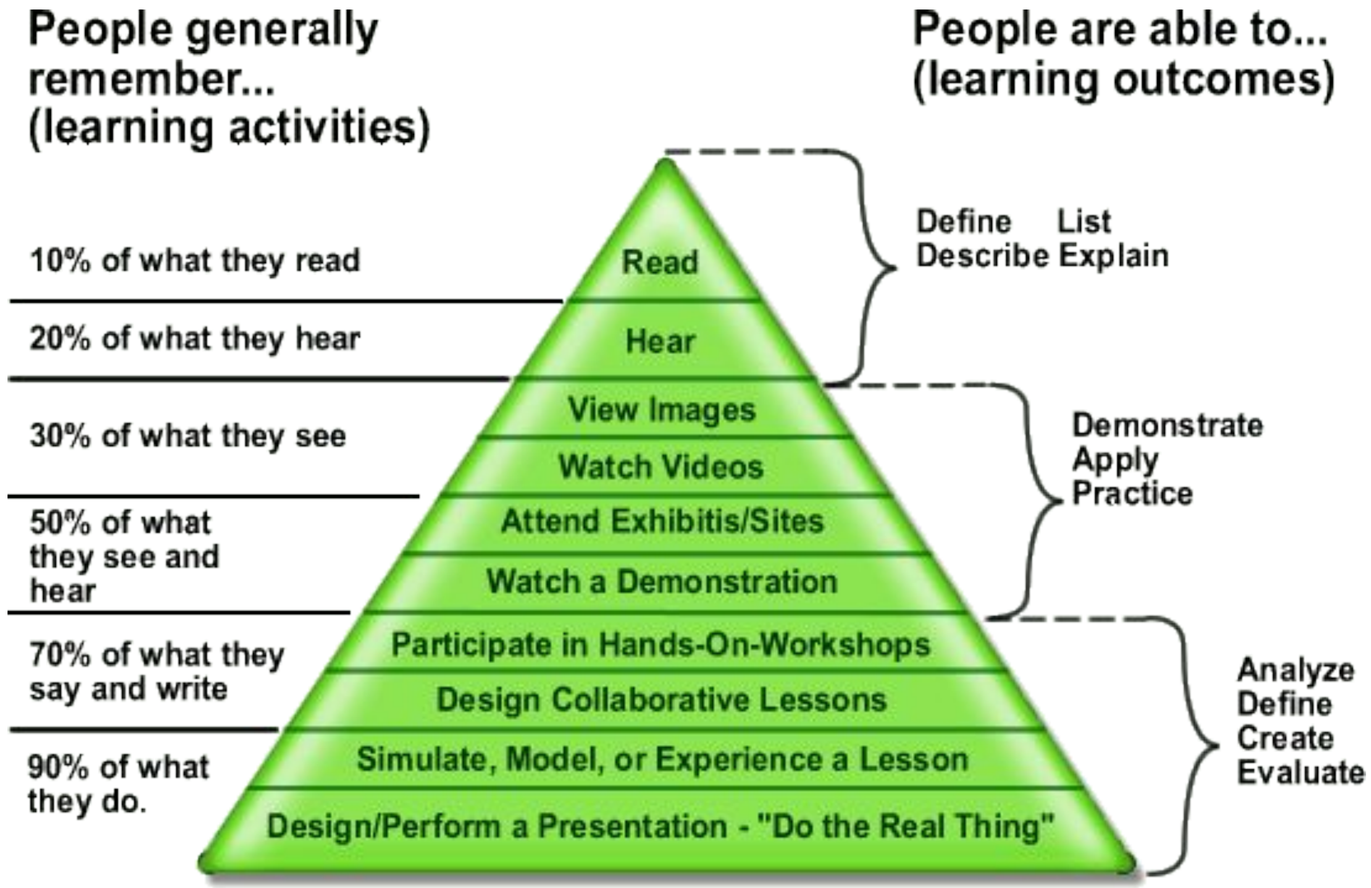
Free Software or Open Source

- Free to use, copy, study, modify, redistribute.
- The source code and/or binary is shared.
- The owner/community or the developer fixes it.
- Personal control, customizability and freedom
- Privacy and security as it is open.

Two heads are better than one!

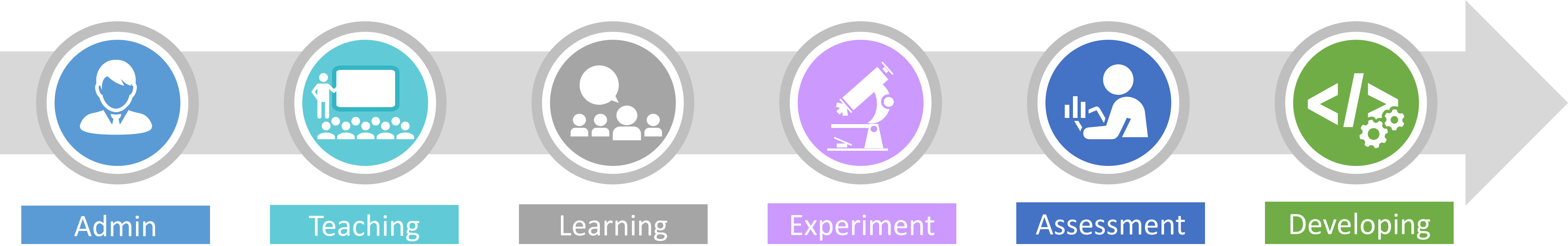
But not a guarantee the security bugs are found and fixed.

EdTech is emulating the Dale's cone


People generally remember... (learning activities)
People are able to... (learning outcomes)
10% of what they read
20% of what they hear
30% of what they see
50% of what they see and hear
70% of what they say and write
90% of what they do.
Read
Hear
View Images
Watch Videos
Attend Exhibitis/Sites
Watch a Demonstration
Participate in Hands-On-Workshops
Design Collaborative Lessons
Simulate, Model, or Experience a Lesson
Design/Perform a Presentation - "Do the Real Thing"
Define List
Describe Explain
Demonstrate
Apply
Practice
Analyze
Define
Create
Evaluate

Src: http://commons.wikimedia.org/wiki/File:Edgar_Dale%27s_cone_of_learning.png

Open Source Software in Education



Admin

- Attendance tracking,
- Class scheduling,
- Student information system,
- Faculty management

Teaching

- Faculty Management System,
- Online classes,
- Video on demand (Swayam, DIKSHA, NPTEL),
- Online whiteboards

Learning

- Learning Management System,
- Knowledge base and references (Vikaspedia, isea, unesdoc, NCERT online textbooks, epathshala),

Experiment

- Simulation labs (olabs,),
- Remote labs

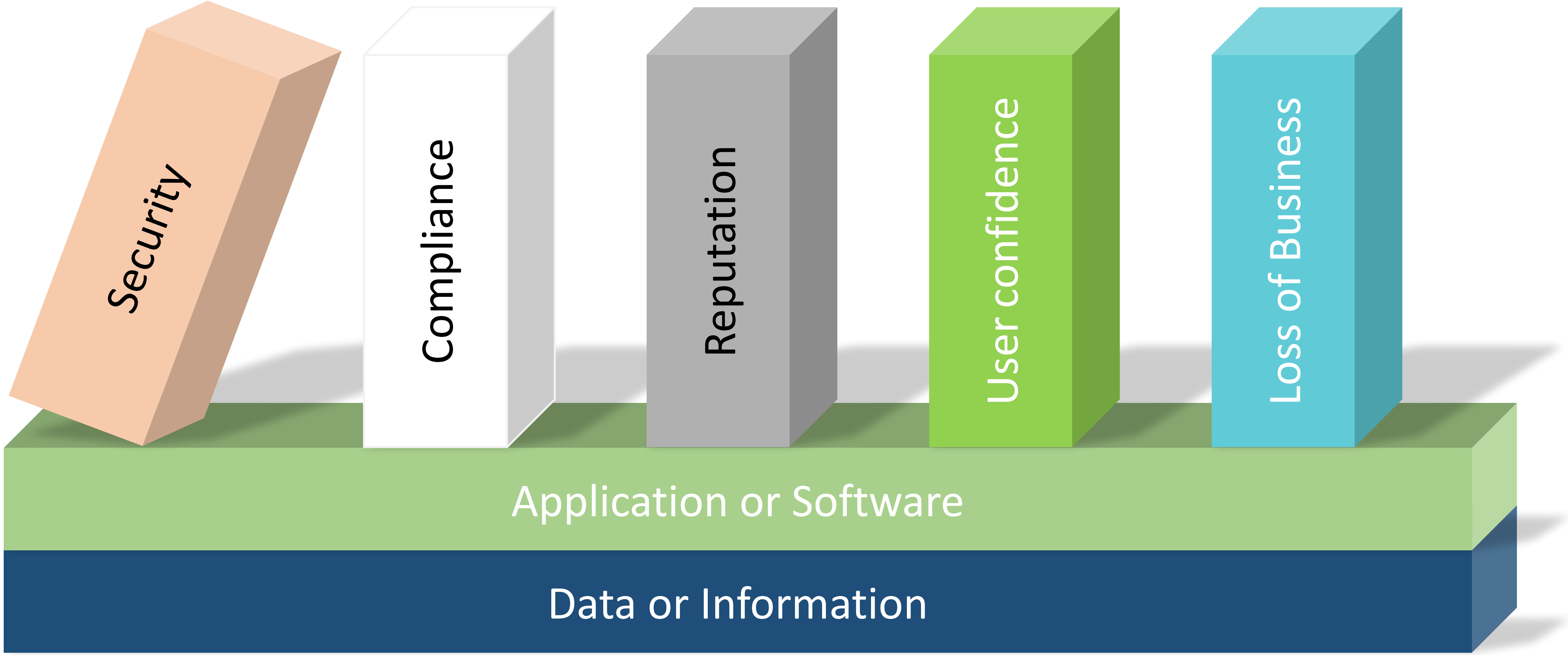
Assessment

- Entrance exams (JEE, NTA, NEET,..),
- Summative assessment (CBSE CCE,..),
- Formative assessment,
- Score evaluation,
- Students progress analysis,

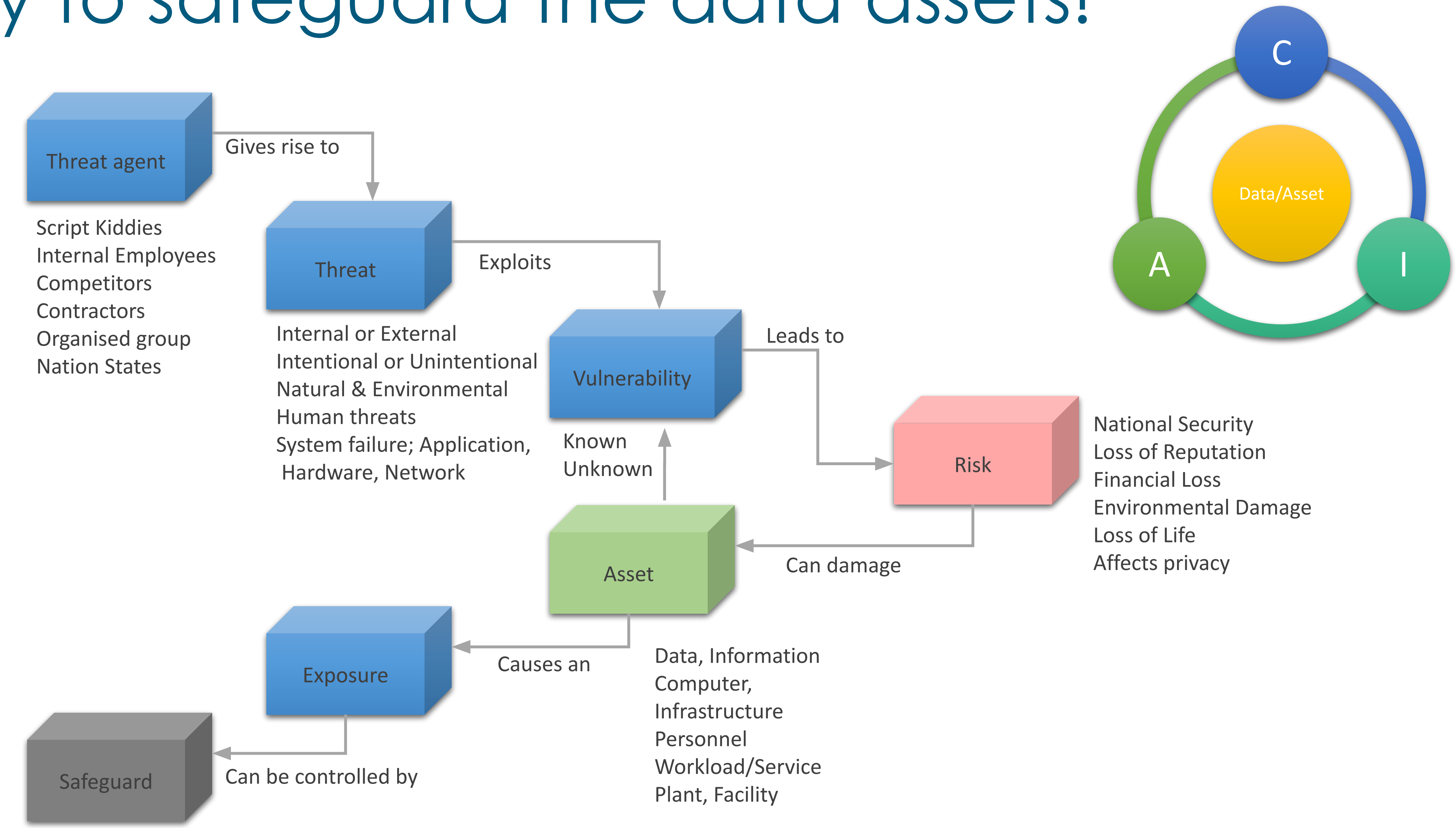
Developing

- School requirement
- Student projects
- Hackathons (Smart India,)

Why is security important



Why to safeguard the data assets!



Threat agent

Script Kiddies
Internal Employees
Competitors
Contractors
Organised group
Nation States

Gives rise to

Threat

Internal or External
Intentional or Unintentional
Natural & Environmental
Human threats
System failure; Application,
Hardware, Network

Exploits

Vulnerability

Known
Unknown

Leads to

Risk

National Security
Loss of Reputation
Financial Loss
Environmental Damage
Loss of Life
Affects privacy

Can damage

Asset

Data, Information
Computer,
Infrastructure
Personnel
Workload/Service
Plant, Facility

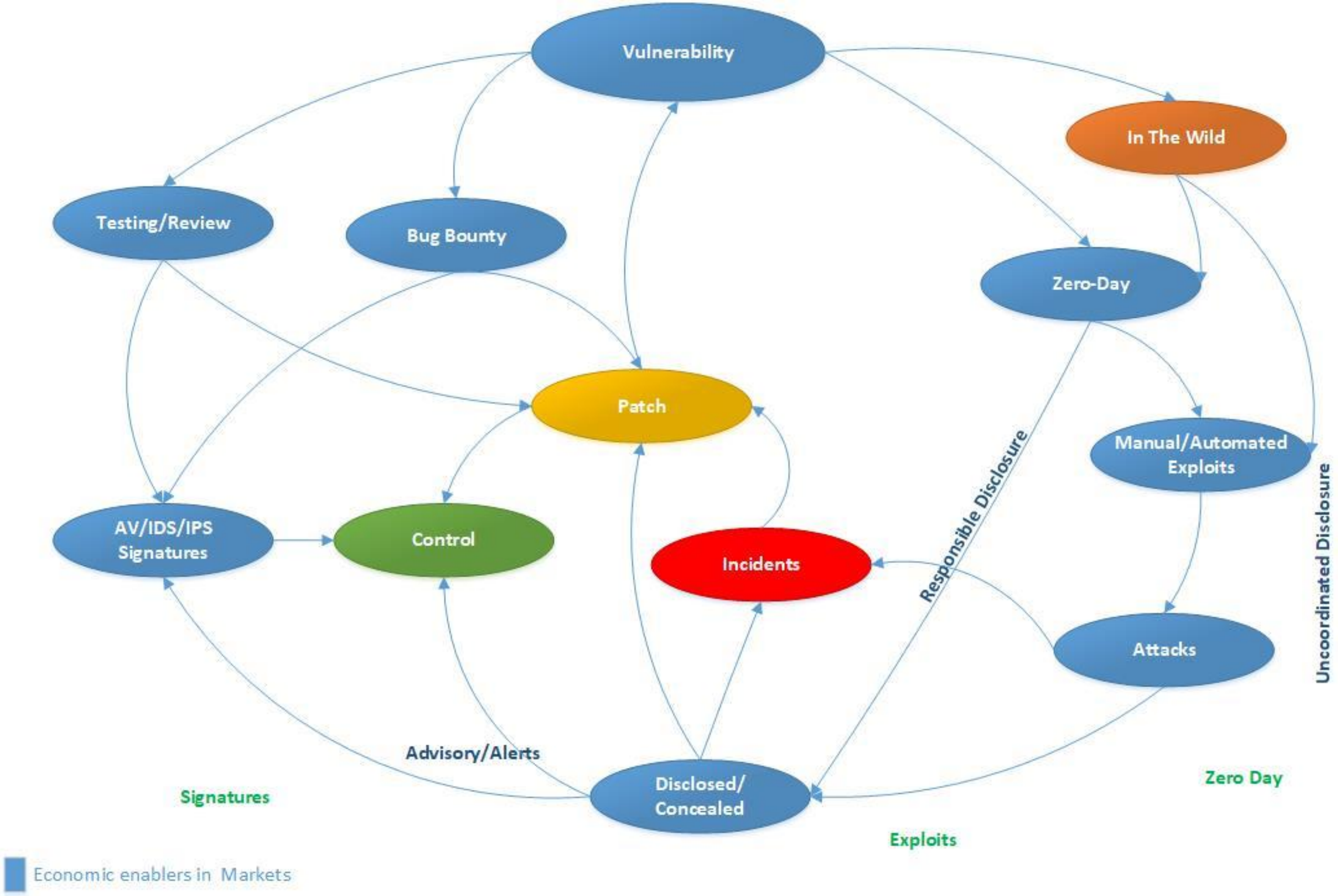
Causes an

Exposure

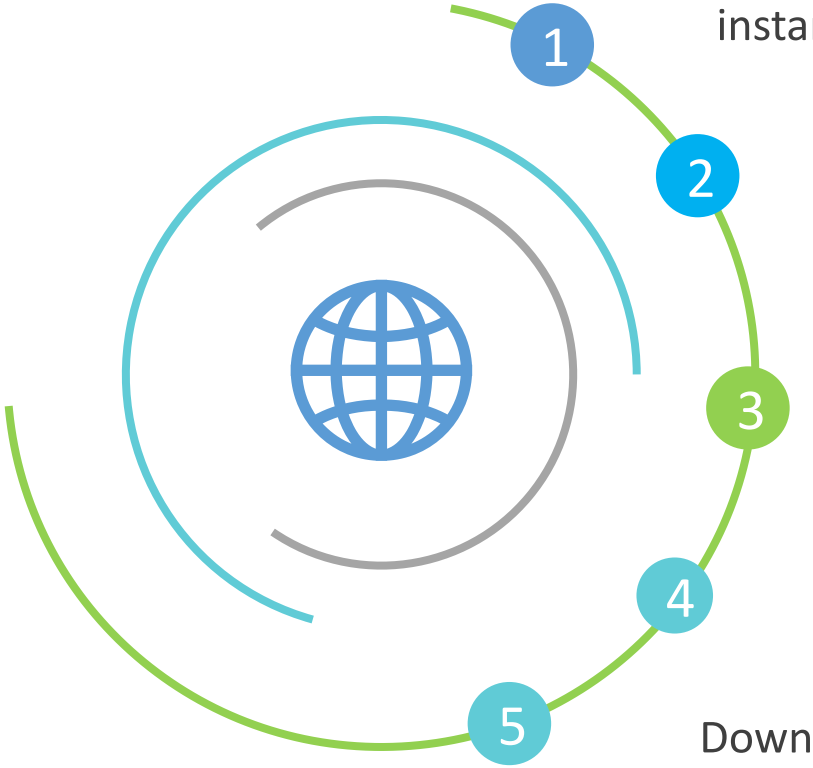
Can be controlled by

Safeguard

The economy around the IA weakness



Security consideration while in virtual labs



Always access the lab website URL, directly. Do not access from any instant messenger, chat forum, news group or SMS.

Do not collect or share unnecessary/irrelevant privacy information;

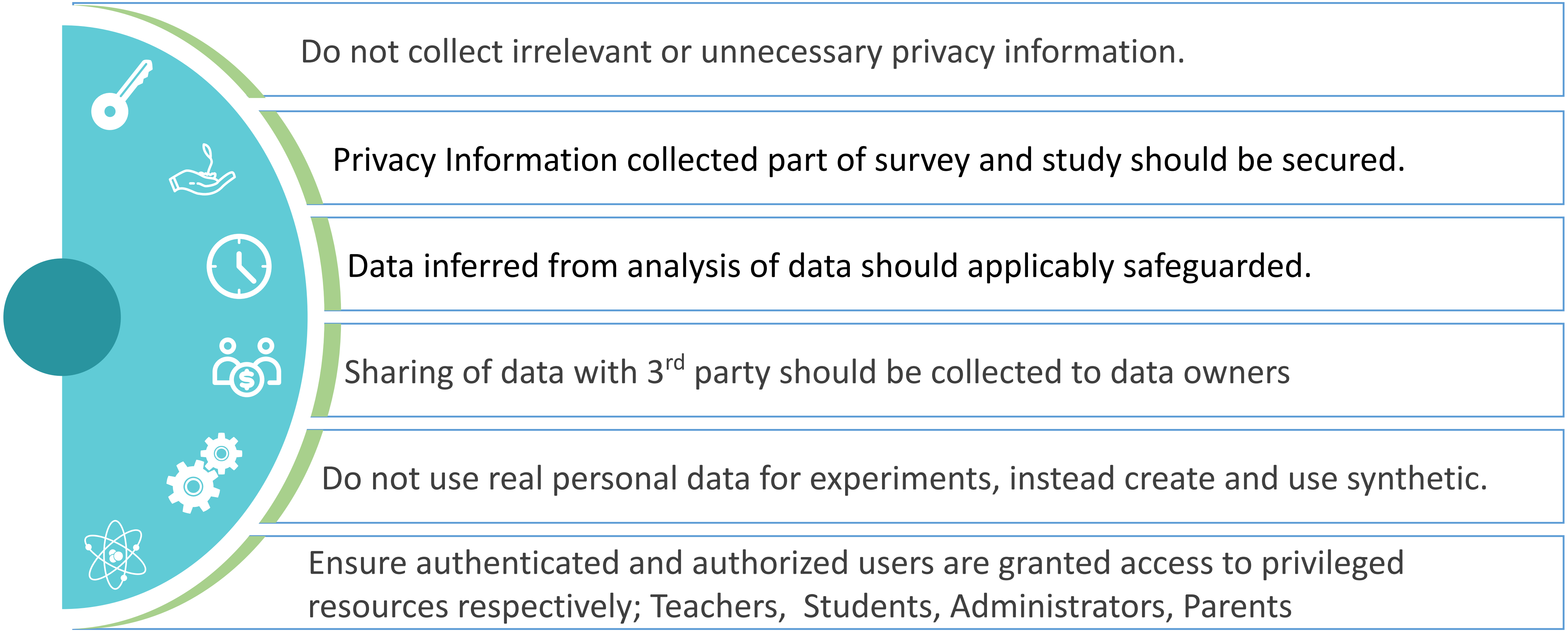
- Exercises
- Practice data
- Real data relevant to an individual violating privacy

Do not click on any unknown links from the chat or discussion forum, that could be a phishing scam.

Disable application sensors using virtual labs on mobile, tablet or laptop when not in use, that may track student activities. Use a different browser for teaching and learning access.

Download and install lab software's from authentic sources.

Secure behaviours as users/experimenters



Do not collect irrelevant or unnecessary privacy information.

Privacy Information collected part of survey and study should be secured.

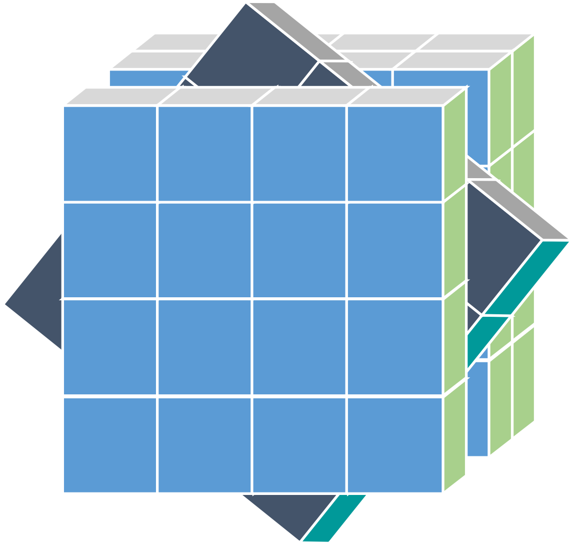
Data inferred from analysis of data should applicably safeguarded.

Sharing of data with 3rd party should be collected to data owners

Do not use real personal data for experiments, instead create and use synthetic.

Ensure authenticated and authorized users are granted access to privileged resources respectively; Teachers, Students, Administrators, Parents

Security consideration in software customisation



PUBLIC DOMAIN

GPLv3 Free Software
Free as in Freedom

open source initiative®

01 Source code or content licencing.

02 Authentication, Authorization and Access Control

03 Data protection at storage and transit.

04 Strong cryptographic algorithm and key management.

05 Secure configuration management.

Secure practices as ideator / developer

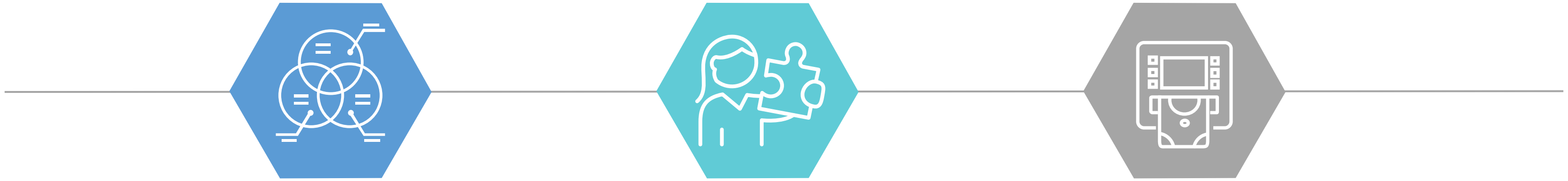
- Secure development lifecycle practices.
- Changes or additions to the code should be through secure development lifecycle practices.
- Should consider

  https://12factor.net/

  OWASP

  https://wiki.sei.cmu.edu/

- Open Education Resource (OER’s), digitized material offered freely and openly for educators, students and learners to teach, learn, develop and research.
- If you choose to release free and open, appropriately license them.



For School

Projects

Hackathon

Changing paradigm

- The virtual world is mapping the physical and biological sphere
- Technology is becoming intrusive

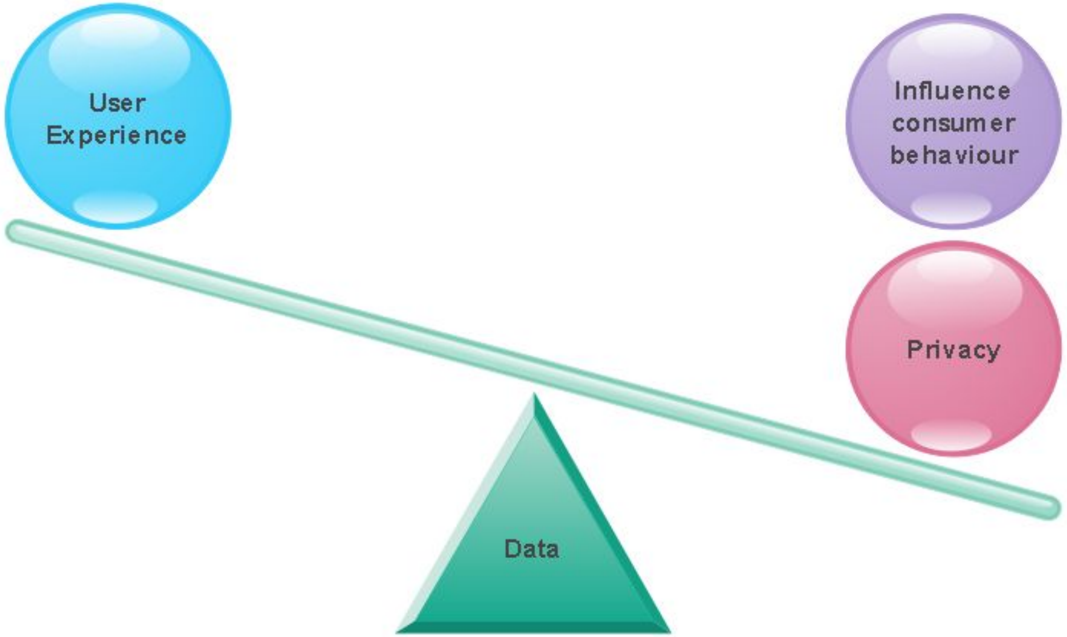
  Fitbit, Crowdsourcing, wearable, implantable

  Convenience vs Privacy

  What if these data are used to design products and services
- Behaviour Influence

  You online activity would reveal your habitual behaviours

  - Browsing history, search terms, location data, contact list, online shopping, Map Navigation, Search Pattern, Comments and Reviews in forums,
- Socio-Economic influence



From the smart alarm that wakes up, fitness band that keep tracks of heart rate, sleep, calorie burn and certain health status, telematics commuting records, electronic calendar alerts, email content information, spending habits, preferred brands, internet browsing activities, TV program choice and everything Comments and Reviews in forums you interact electronically would create an electronic signature when collated or fragmented.

Education software usage & data protection

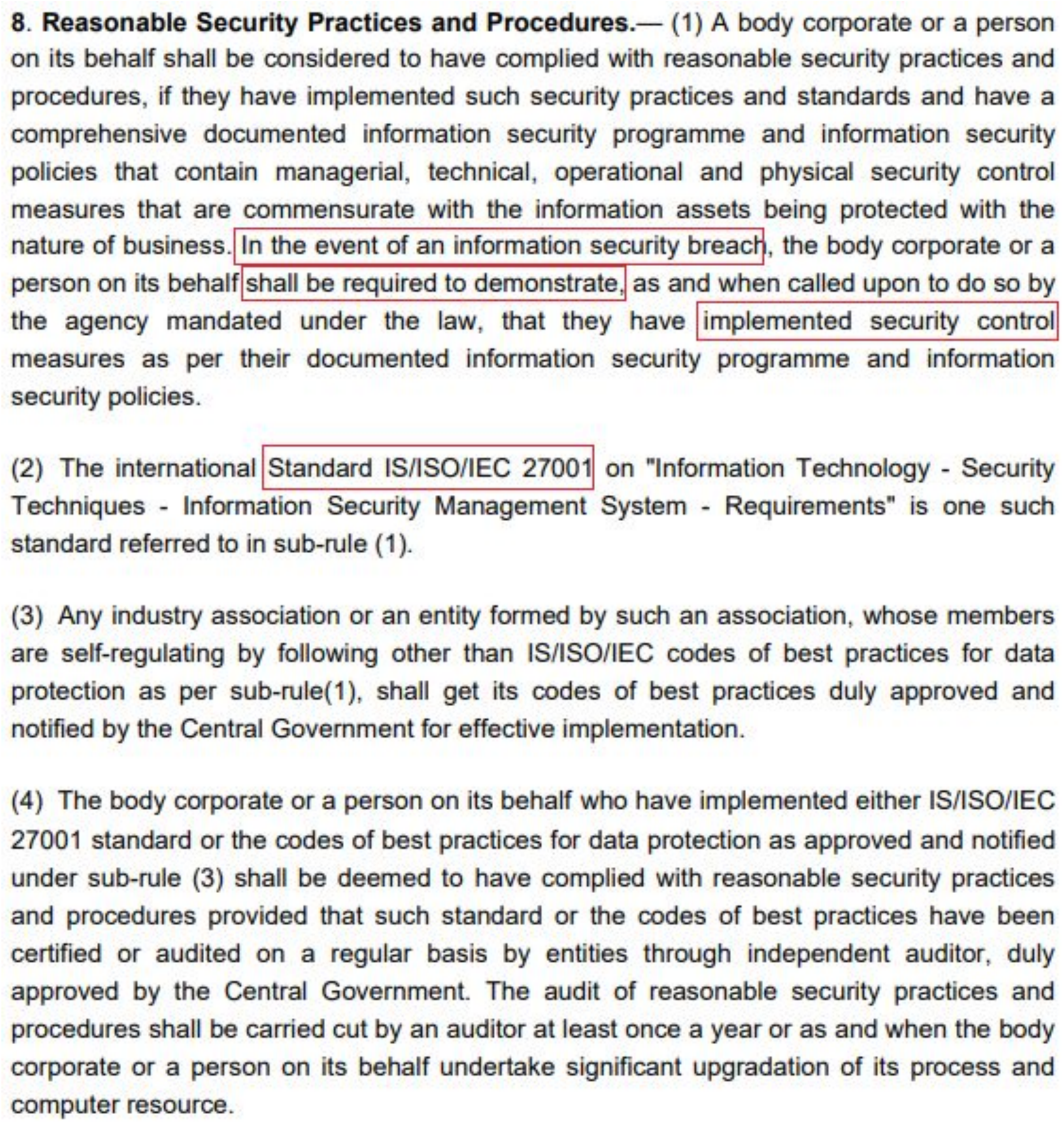
YES

Upon, Failure of due diligence and due care…

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates is negligent in implementing and maintain reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

GSR 313 (E)

Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011



8. Reasonable Security Practices and Procedures.— (1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

(2) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

Thank You

rakesht@cdac.in | www.cdac.in

धन्यवाद आभार આભાર ਧੰਨਵਾਦ ধন্যবাদ நன்றி നന്ദി നേരുന്നു