



# CYBER SECURITY



# Open Source

# Open Source

In production and development, open source is a philosophy or a concept that promotes free redistribution and access to a product's design or ideas and implementation details.

- Open as in Free
- Open as in access
- Open as in over time
- Open as in reuse and change
- Open as in any location and for anyone

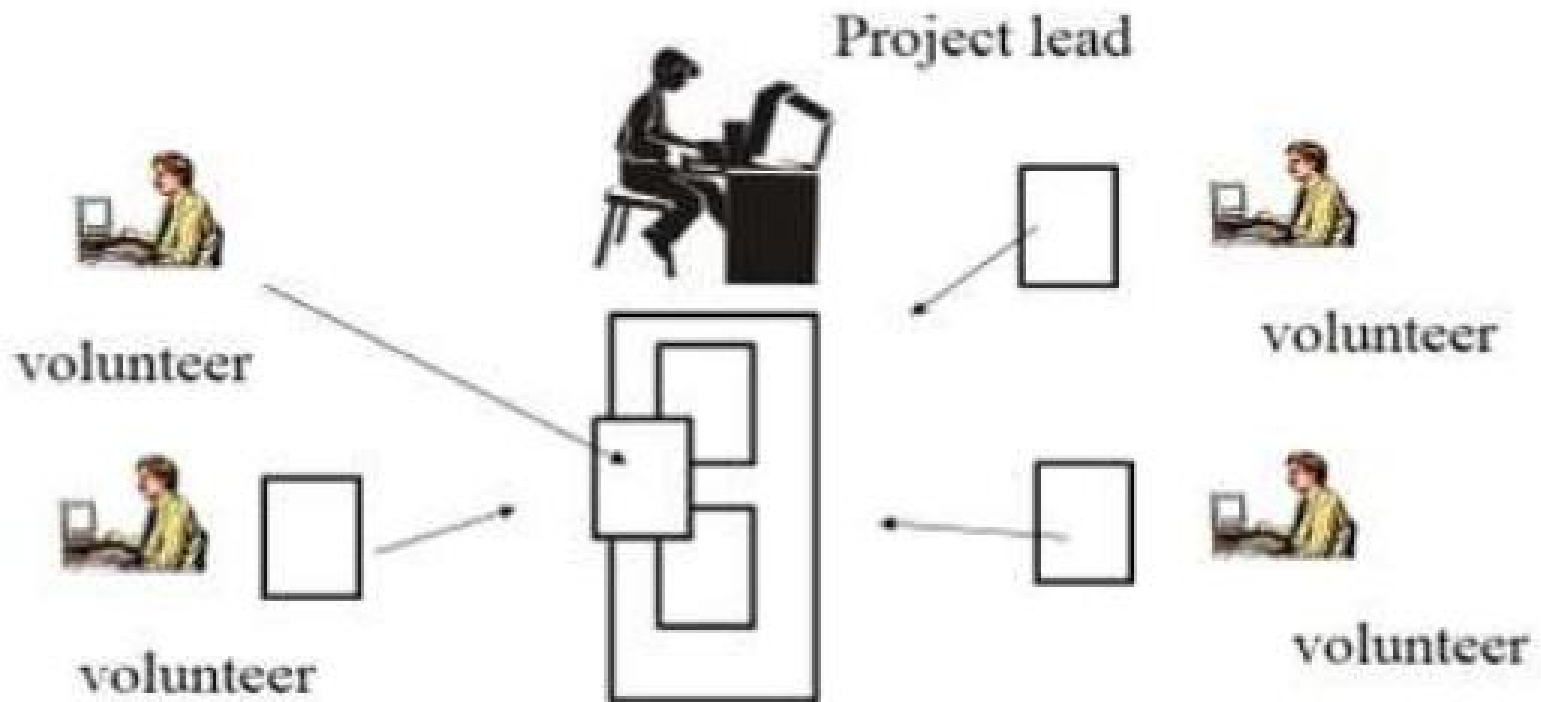


# Open Source Software

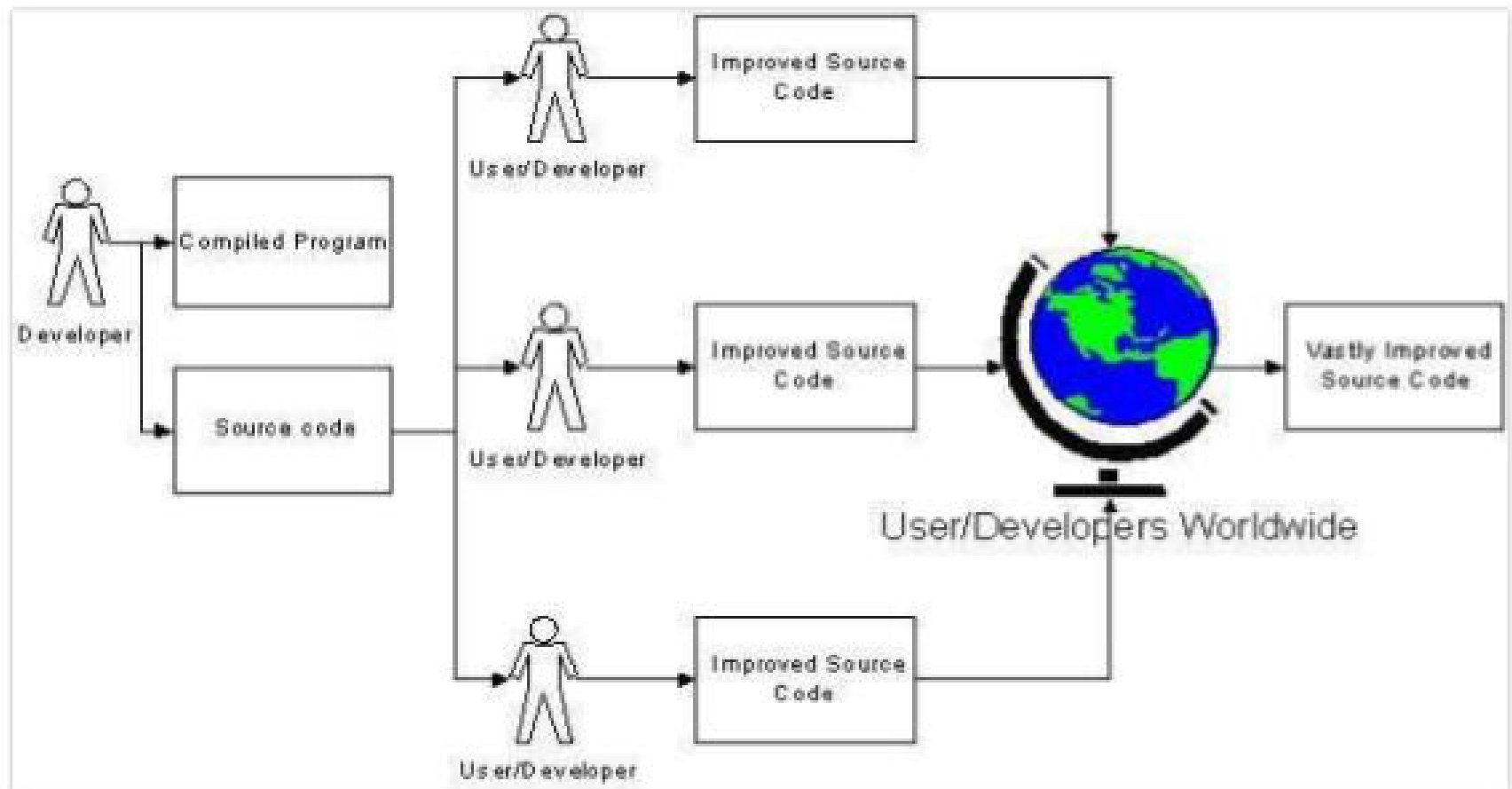
- Developed either by an individual /group or a project
- Community / participative development concept
- Codes are publicly available
- Usually comes with an open source license
- Usually free or restrictive usage permission
- License must not restrict other software
- Integrity of developers' source code
- Cheaper

Open source software Vs Free software

# OPEN SOURCE DEVELOPMENT MODEL



# HOW OPEN SOURCE WORKS ?



# Open Source Software

Availability : Everywhere across all sectors

- Application software
- System software
- Tools
- Security
- Appliances
- Plant automation
- ML & AI
- New and emerging technologies

# EXAMPLES

- Linux based OS designed primarily for touch screen based mobile devices. Released under apache license.
- Over 7 lakh apps in Google play store, 25 bn downloads and 750 mn devices around world
- <http://source.android.com>

## Application software :

- 7-Zip
- Eclipse
- GIMP
- Chromium
- Blender
- Mozilla Firefox
- Open Office

## Open

- Android
- Linux
- FreeBSD
- ReactOS
- Haiku
- FreeDOS

## Language :

- Perl
- PHP
- Python
- Ruby
- PHDL
- Prolog



# EXAMPLES OF OPEN SOURCE

- Developed by Richard Stallman (1983) as part of GNU project in FSF.
- >90% super-computer used Linux, powers around 4.8% of todays computer
- Market share:
- Desktop: 8.79%, Mobile: 39%, tablet: 39%

## Application :

- 7-Zip
- Eclipse
- GIMP
- Chromium
- Blender
- Mozilla Firefox
- Open Office

- Android
- Linux
- FreeBSD
- ReactOS
- Haiku
- FreeDOS

## Programming Language :

- Perl
- PHP
- Python
- Ruby
- PHDL
- Prolog

# EXAMPLES OF OPEN SOURCE

## Server Software:



# OPEN SOURCE DIGITAL CONTENT

## Wikimedia Foundation

Wikimedia is owned and operated by the Wikimedia Foundation, a non-profit foundation dedicated to bringing free content to the world. The various Wikimedia projects are listed below:



a multilingual free  
encyclopedia  
**Wiktionary**  
[ˈwɪkʃənəri] n.,  
a wiki-based Open  
Content dictionary  
WIKIMEDIA FOUNDAION



# Myth about Open Source

FOSS : Free and Open Source Software

- FOSS is 'Free'
- FOSS is not reliable or supported
- Making a software open source, anyone can ch
- Open Source License is too liberal
- Volunteer will fix all the problems of FOSS for f





# Security

# Layers of Vulnerability

- Public facing set-up
- Network
- Data Centre
- Server
- Software
- Other connected systems (IOT, IIOT, Automobile, plant etc)

# Cyber Security

As per ITAA 2008:

Protecting information, equipment, devices, computer, computer resource, communication device and information stored there-in from unauthorized

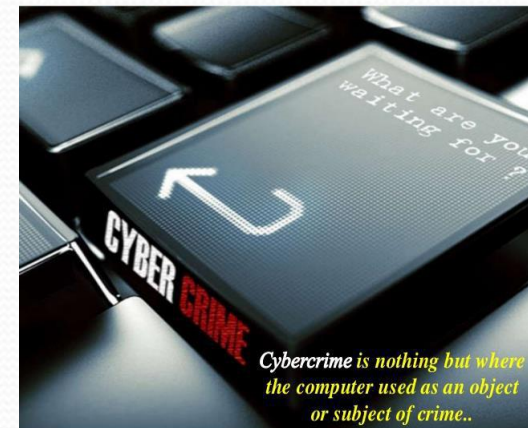
- Access
- Use
- Disclosure
- Disruption



# Cyber Crimes

***Criminal activities carried out by means of computers or the as Cyber Crime and It's various types are :***

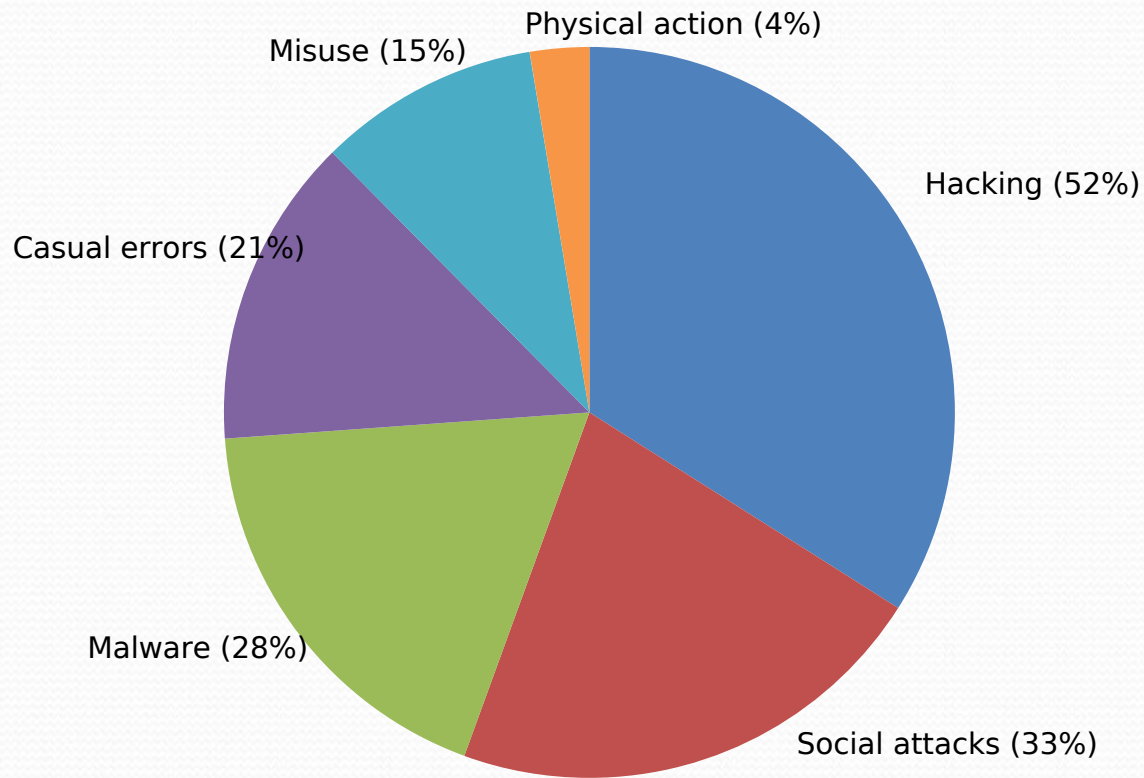
- DoS & DDoS
- Identity Theft
- Phishing and Spear Phishing
- Virus Dissemination
- Cyber terrorism
- SQL injection and Cross-site scripting
- Software piracy
- State sponsored attack





# Verizon DBIR Report - 2019

What tactics are utilized ?



■ Hacking

■ Social attack

■ Malware

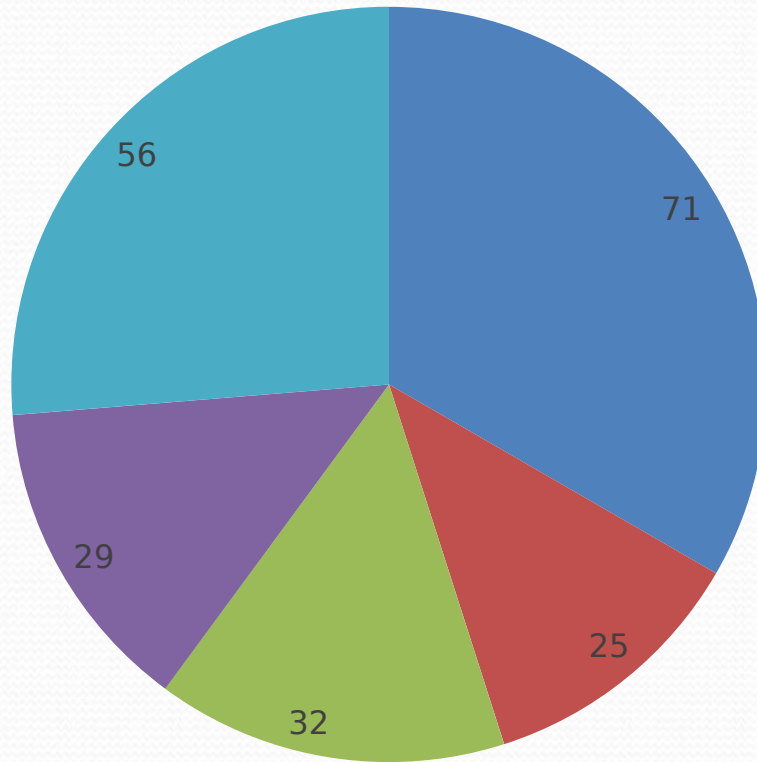
■ Casual errors

■ Misuse by Authorized users

■ Physical actions

# Verizon DBIR Report - 2019

What are the objectives ?



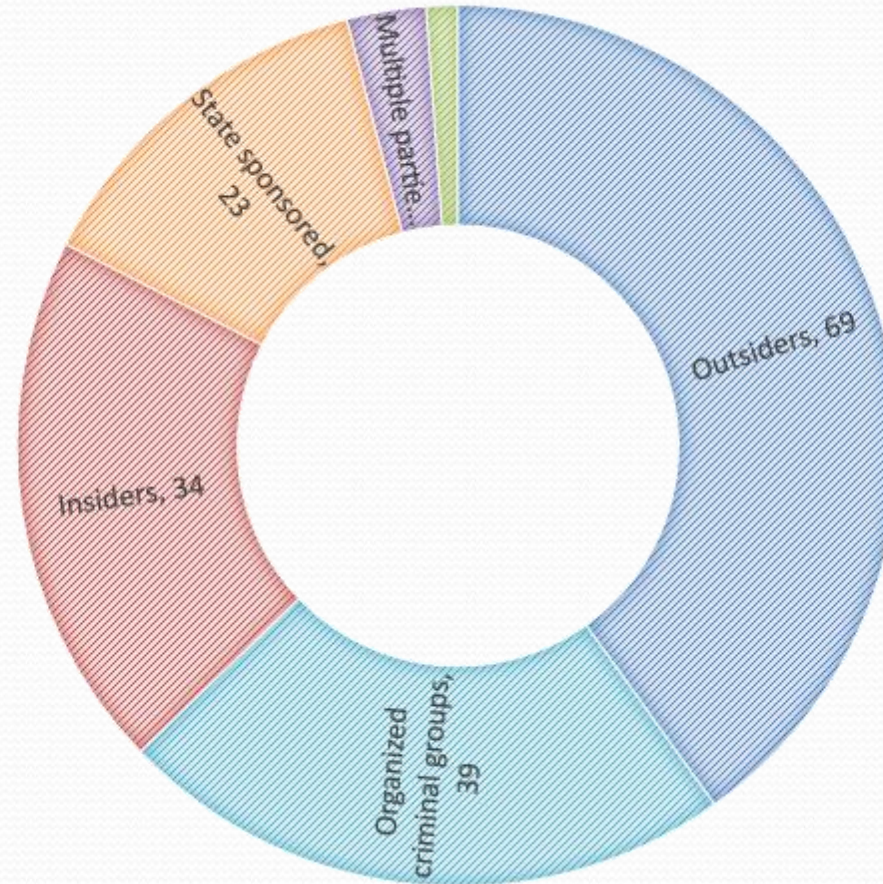
■ Financially motivated ■ Espionage ■ Phishing ■ Identity theft ■ Took months to detect



# Verizon DBIR Report - 2019

Who's behind the breaches ?

■ Outsiders ■ Insiders ■ Partners ■ Multiple parties ■ Organized criminal groups ■ State sponsored



# Some reported attack, Global - 2019

- 'Silence' hackers steal more than \$3 million from banks in Bangladesh, Sri Lanka and Kyrgyzstan (unknown)
- Hackers steal names & Social Security numbers from Maryland Department of Labour (78,000)
- State-sponsored hackers breach Greece's top-level domain registrar (unknown)
- Chinese job recruiting site hacked, with CVs for sale on dark web(160000)



# Some reported attack, Global - 2019

- Los Angeles Co. Department of Health Services email hacked exposing patient data (14,591)
- Japanese cryptocurrency exchange Bitpoint loses \$32m in cyber attack (unknown)
- University of Alabama discovers 10-year-old account breach (1,400)
- Data at Bahamas Ministry of Tourism corrupted by virus (unknown)
- Capital One says credit card applicants' data stolen (100 million)

# Some reported attack, India - 2019

- India Ranked Highest in IoT Cybersecurity Attacks Last Quarter: (News18)
- 1,852 Cyber Attacks Hit India Each Minute Last Year; Mumbai, Delhi Most Affected (News18)
- India sees dramatic rise in cyber attacks post-Kashmir decision (mint)
- India is one of the most vulnerable nations in the world when it comes to cyber-attacks (NASSCOM)



# Some security breaches in the past

- Equifax data leak (2017)-US Cr Bureau, 143 mn data
- Yahoo data leak (2013-14)-1 bn data
- Stuxnet (2010)-Iran, Ukraine
- Marriot International (2014-18), 500 mn data
- Heartland Payment System (2008), 100 mn

# Open Source security challenges

- Hackers can use the National Vulnerability Database (NVDB) for exploits and use those to their advantage by targeting organizations that are slow to patch the applications that may be dependent on open source projects with recent vulnerabilities
- Time to respond to a reported vulnerability, quality of patch
- Hackers are also exploring possible vulnerabilities
- Herculean task if the software is being maintained by the organizations themselves'
- Availability of skilled resources (Developing and retaining)
- Version / configuration management
- Error free version
- No contract protection
- Risk of infringement (3<sup>rd</sup> party IP)
- User conveniences

**These possess more challenges for open source based critical applications**



# Recommended steps

Implement security at all levels

Gateway level (Public facing)

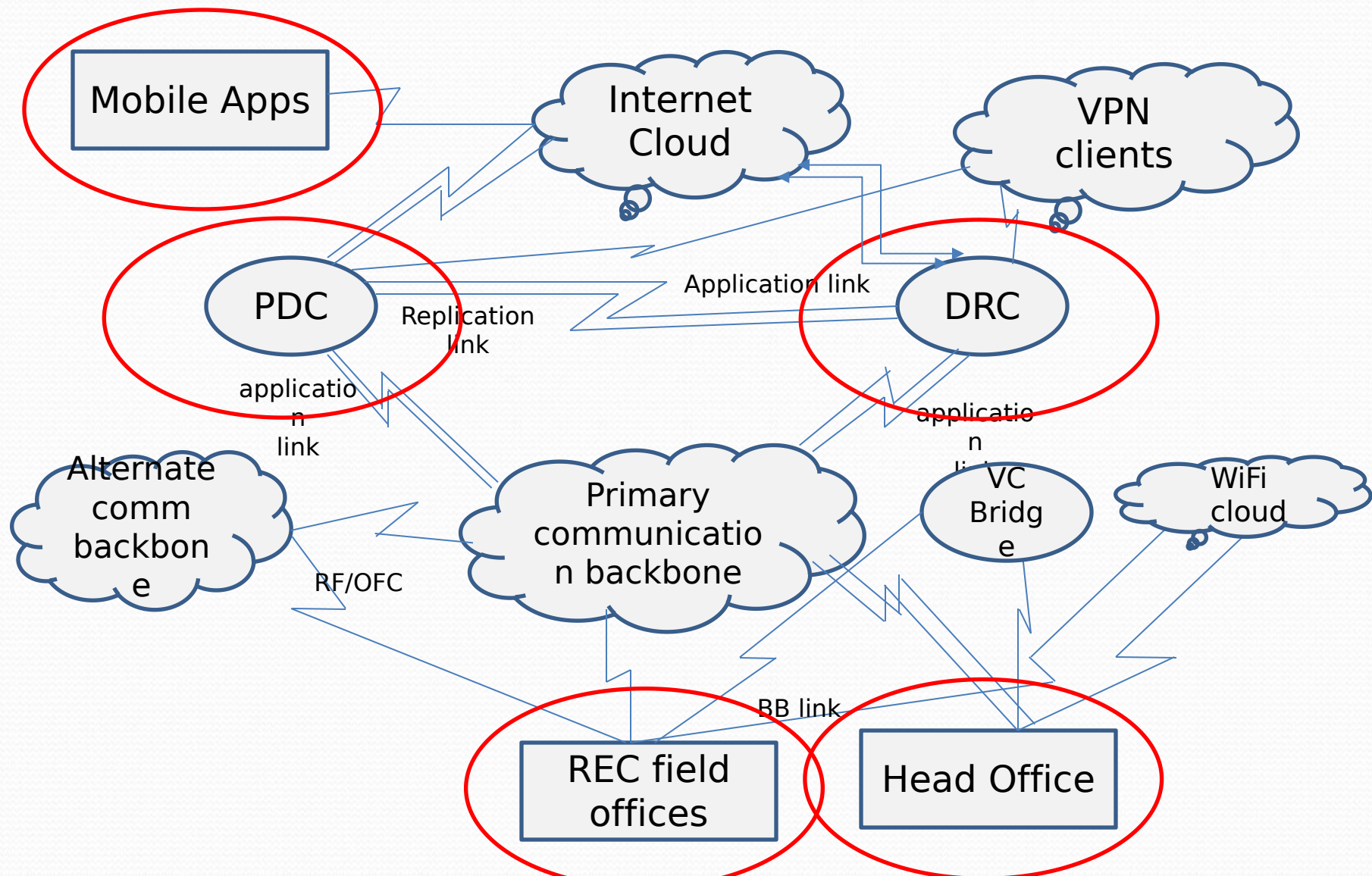
Internal network level

Data Centre level (Router, Switch, FW, IPS,  
OS, Application, Database)

Individual office level (perimeter)

End-user level (Anti-virus, FW, DLP)

# Security Layers



# Recommended steps

- Introduce coding standard

  - Structured

  - use comments freely

  - Close unused ports

  - optimized coding

  - Apply patch regularly

- Awareness creation among users (training, self learning CD, communication)

- Continuous audit

  - PT, VA

  - White & Black box testing audit

  - Separate security testing for codes

  - QA

- Encryption

- Backup



# Recommended steps

Compliance to security guidelines and standard

ITAA 2008

NCSP 2013

RBI Guidelines

IRDA guidelines

ISO 27001

CoBIT

**CMMI**

Use 3 factor authentication

Use SSL, DSC

URL Filtering

Basic pre-caution

Setting up infrastructure for prevention of eventualities, like:

DOS/DDOS attack

Ransomware attack

Social Engg attack

Red Team exercise

```

/**
 * Simple HelloButton() method.
 * @version 1.0
 * @author john doe <doe.j@example.com>
 */
HelloButton()
{
    JButton hello = new JButton( "Hello, wor
hello.addActionListener( new HelloBtnList

// use the JFrame type until support for t
// new component is finished
JFrame frame = new JFrame( "Hello Button"
Container pane = frame.getContentPane();
pane.add( hello );
frame.pack();
frame.show();           // display the fra
}

```

```

HelloButton()
{
    JButton hello = new
JButton( "Hello, wor
    hello.addActionListener(New
HelloBtnList

    JFrame frame = new JFrame( "Hello
Button"
    Container pane =
frame.getContentPane();
    Pane.add( hello );
    Frame.pack();
    Frame.show();
}

```



# Recommended steps

Leading causes of data breaches often involve workforce mistakes. Malicious outsiders often get in because they trick people through phishing and social engineering.

Educate the workforce! Train them once, train them twice, train them thrice. Make them care.

Recommendation - Grant min access privilege, implement 3 factor authentication, IPS/FW, AV

Password: Letters-6 min, UC+LC letters-6 hrs, UC+LC+Num - 25 days, All combination - 2 years

## Breaching statistics

67% - Breached from servers

76% - Breached using weak control of the system

97% - Preventable through simple security



# Types of Security testing

Black box testing

White box testing

Penetration testing

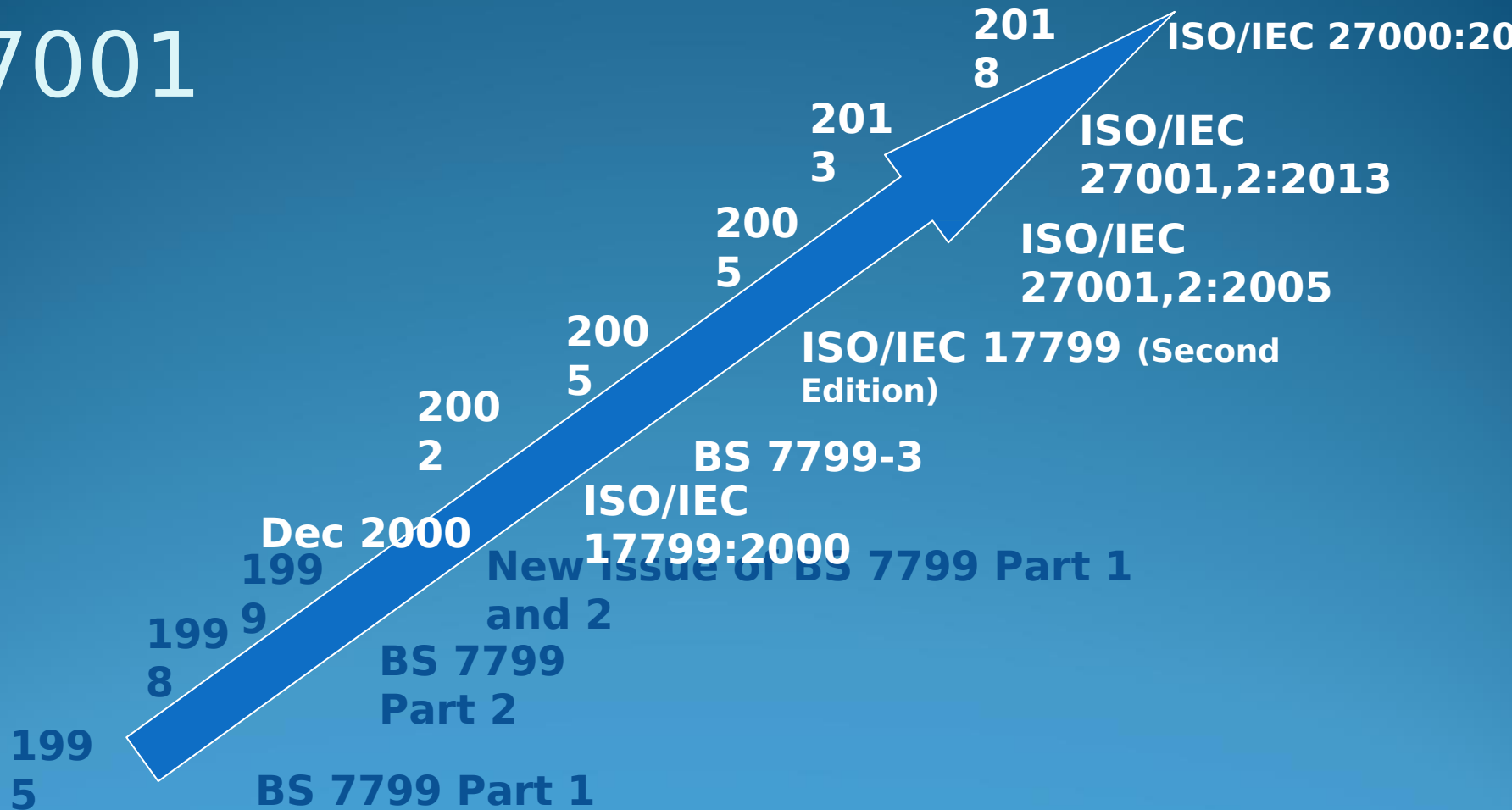
Compliance testing

Load testing

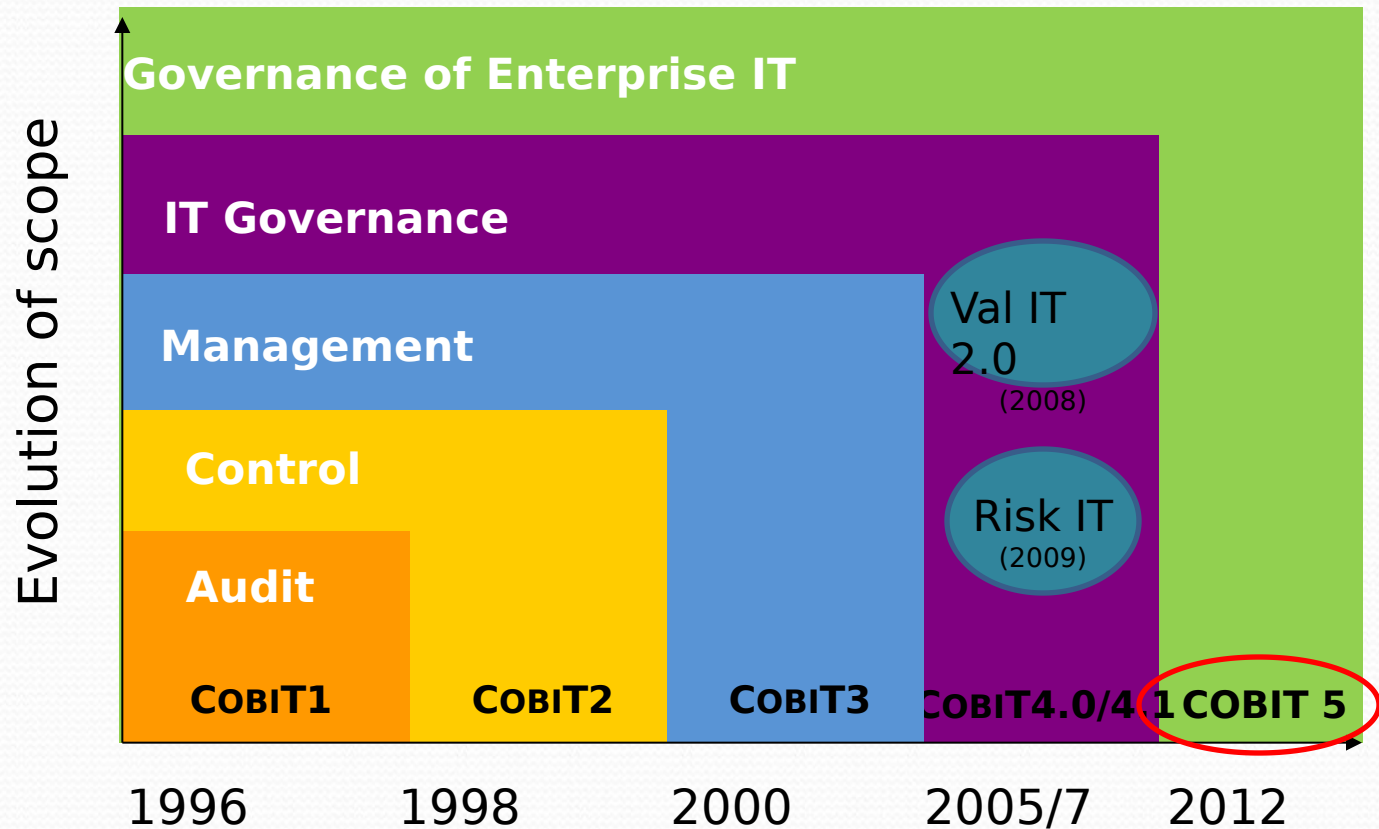
OWASP testing guidelines

Manual

# Evolution of ISO 27001




# Evolution of COBIT standard



An business framework from ISACA, at [www.isaca.org/cobit](http://www.isaca.org/cobit)





Q &  
A