ENTERPRISE CYBER SECURITY

Course Objectives

- Learn the fundamentals of cryptography.
- Learn the key management techniques and authentication approaches.
- Explore the network and transport layer security techniques.
- Understand the application layer security standards.
- Learn the real time security practices.

Course Outcomes

- Understanding the core concepts and importance of cybersecurity in organizational settings.
- Acquire the knowledge common network attacks and deploy appropriate security measures.
- Implement encryption and secure communication protocols for data integrity and confidentiality.
- Deploy and manage Intrusion Detection and Prevention Systems for threat detection.
- Identify and mitigate common web application vulnerabilities.
- Conduct penetration tests to evaluate the security posture of web applications.

Unit-1

INTRODUCTION TO CYBERSECURITY

- Cyber Security
- Need of Cybersecurity in Organizations
- CIA Triad
- Confidentiality, Integrity, Availability
- Reason for Cyber Crime
- Need for Cyber Security
- History of Cyber Crime; Cybercriminals
- Classification of Cybercrimes
- A Global Perspective on Cyber Crimes; Cyber Laws
- The Indian IT Act
- Cybercrime and Punishment.

Module 2

NETWORK SECURITY BASICS

- Network Security Concepts
- Basics of Networks
- Common Types of Network Attacks
- Introduction to Firewalls
- Types of Firewalls
- IDS/IPS
- Virtual Private Networks (VPN's)
- Secure configuration and management of network devices.
- Case Study: Install Kali Linux on Virtual box.

Module 3

SECURE COMMUNICATION PROTOCOLS

- Encryption Principles
- Cryptography, Cryptanalysis, Feistel Cipher Structure.
- Block Encryption algorithms: DES, triple DES, and AES.
- Transport Level Security: Secure Sockets Layer (SSL), Transport Layer Security
- Electronic Mail Security
- Pretty Good Privacy (PGP), S/MIME
- Securing wireless networks: WPA, WPA2, WPA3

Module 4

INTRUSION DETECTION AND PREVENTION SYSTEMS

- IDPS
- Need of Intrusion Detection Systems in Cyber Security
- Types of IDPS: Network-based and Host-based
- Configuring and Managing IDPS for threat detection using Honeypots
- Case Study: Setup a honey pot and monitor the honey pot on network

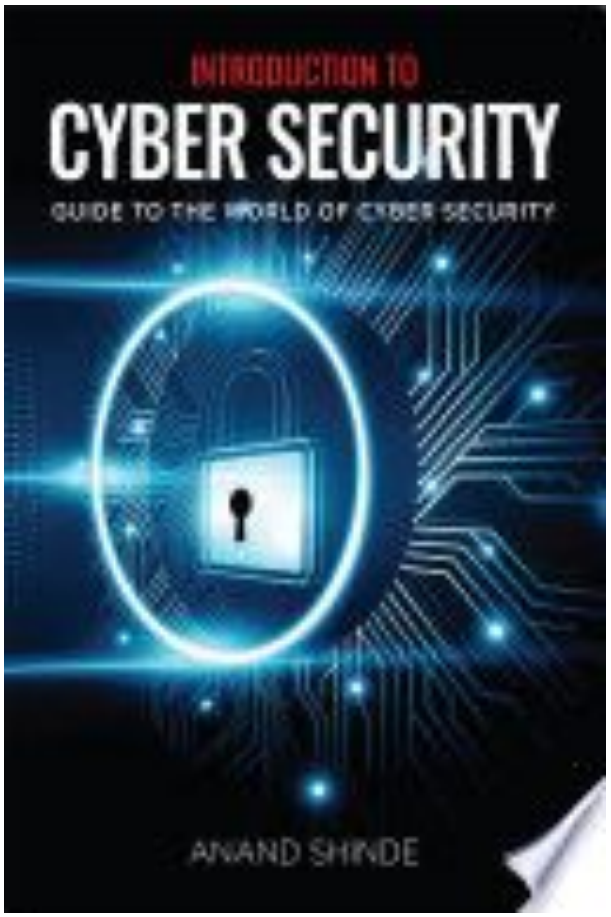
Module 5

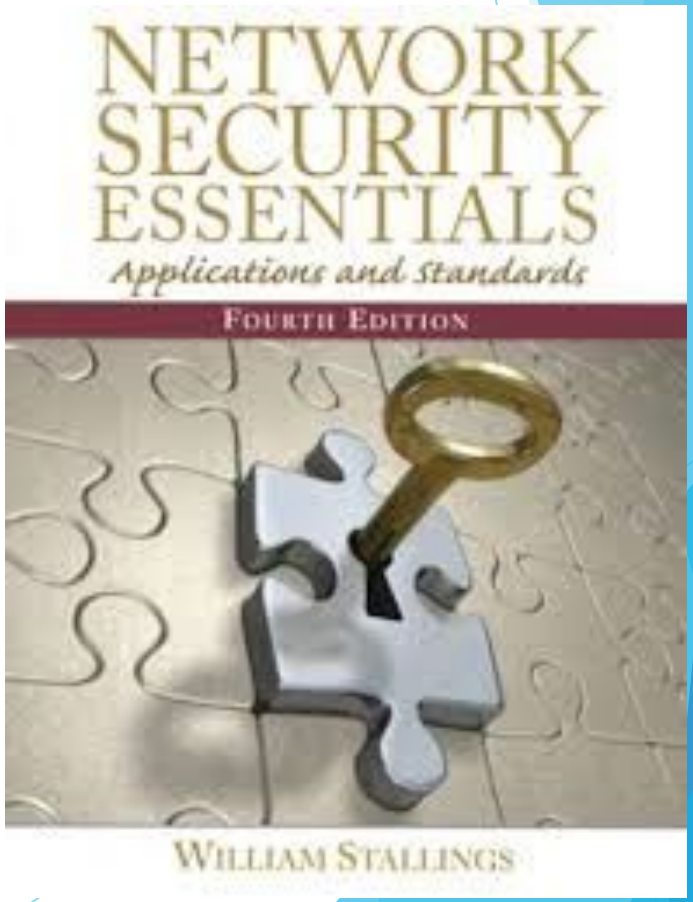
WEB APPLICATION SECURITY

- Introduction to Web Application Vulnerabilities
- Cross Site Scripting (XSS)
- SQL injection- Denial of Service (DoS)
- Web Application Testing
- Types of Penetration Tests
- OWASP and OWASP Top.

Text Books

- Anand Shinde, “Introduction to Cyber Security Guide to the World of Cyber Security”, Notion Press, 2021.
- Network Security Essentials (Applications and Standards) by William Stallings Pearson Education, 2018.

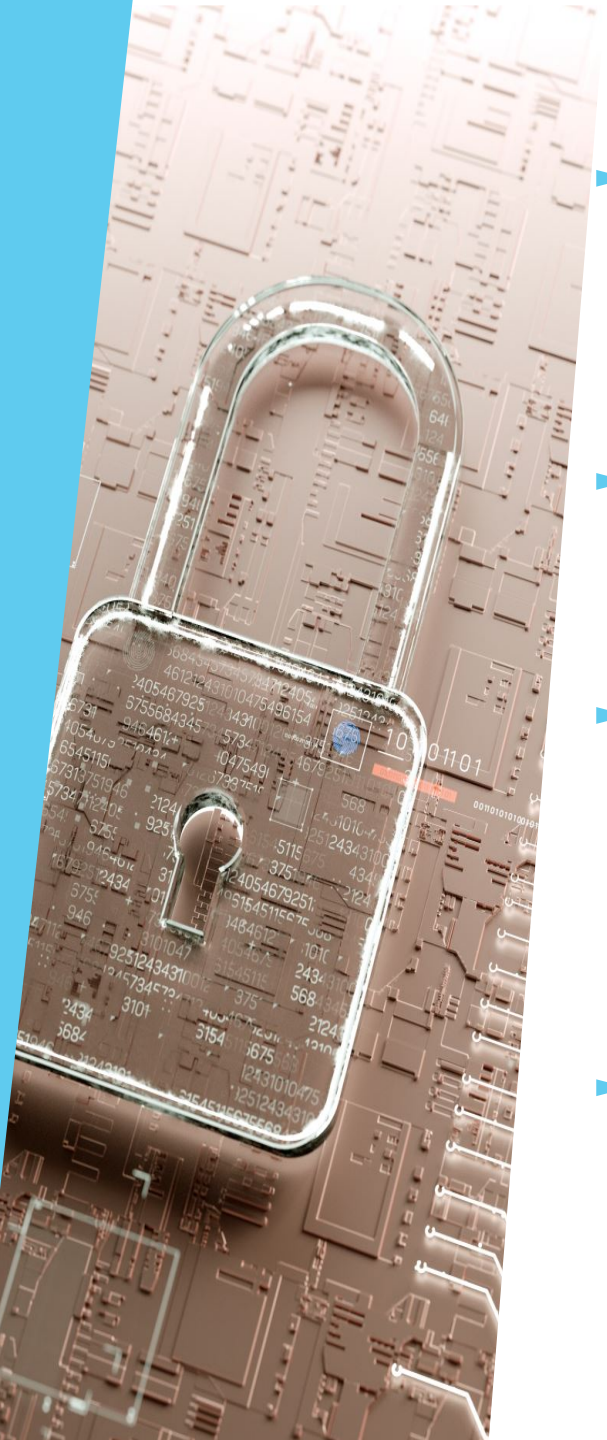




Reference Books

- William Stallings, "Cryptography and Network Security - Principles and Practice", Seventh Edition, Pearson Education, 2017.
- Ravi Das and Greg Johnson, “Testing and Securing Web Applications”, 2021.
- Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O’Reilly Media, Inc, 2020.

Cyber security



What is Cybersecurity?

- The term cyber security is used to refer to the security offered through on-line services to protect your online information.
- Cyber Security and Information Security differs only in its response and Reduction/Prevention.
- Cyber security encompasses all aspects of security viz., Physical, Technical, Environmental, Regulations and Compliance including Third Parties involved in delivering an objective
- With an increasing amount of people getting connected to Internet, the security threats that cause massive harm are increasing also

Need For Cybersecurity

Our world today is ruled by technology and we can't do without it at all. From booking our flight tickets, to catching up with an old friend, technology plays an important role in it.

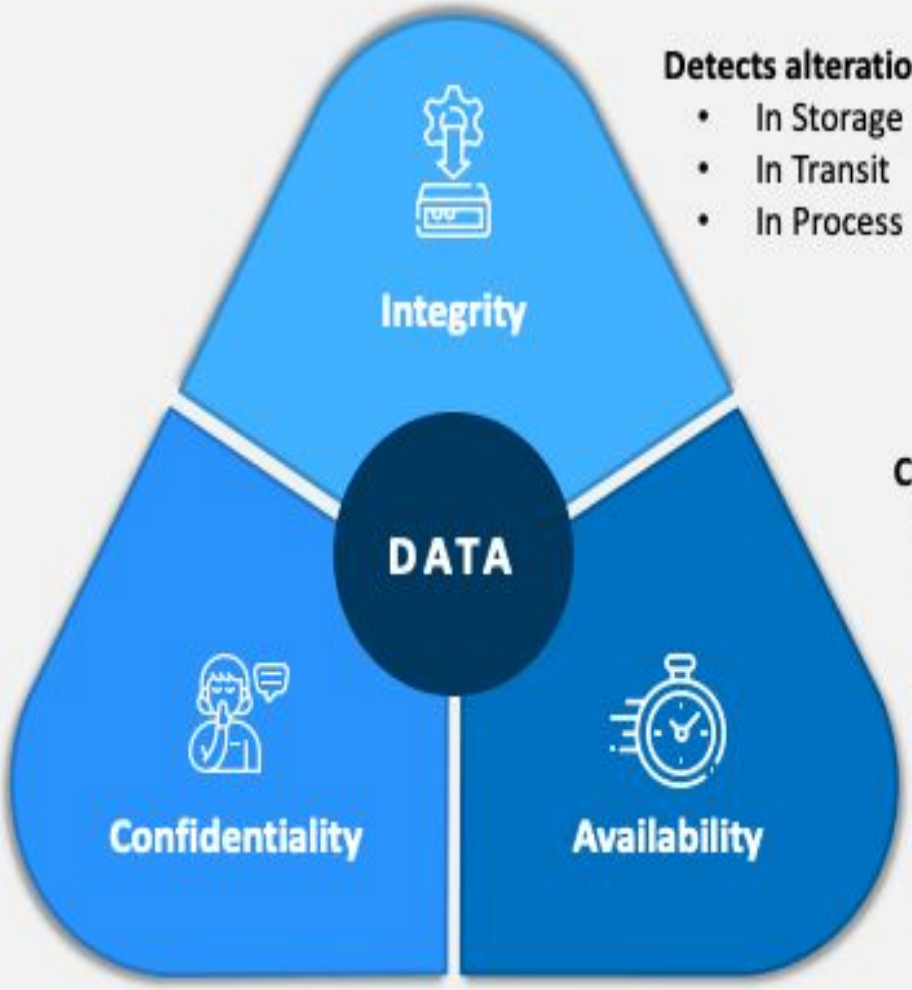
However, the same technology may expose you when it's vulnerable and could lead to loss of essential data. Cyber security, alongside physical commercial security has thus, slowly and steadily, become one of the most important topics in the business industry to be talked about.

Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.

Need For Cybersecurity

- Cyber security becomes important as Business are being carried now on Network of Networks. Computer networks have always been the target of criminals, and it is likely that the danger of cyber security breaches will only increase in the future as these networks expand, but there are sensible precautions that organizations can take to minimize losses from those who seek to do harm.

CIA TRAID



Detects alteration that has occurred

- In Storage
- In Transit
- In Process

Protection From

- Unauthorized access
- Unauthorized Use
- Disclosure

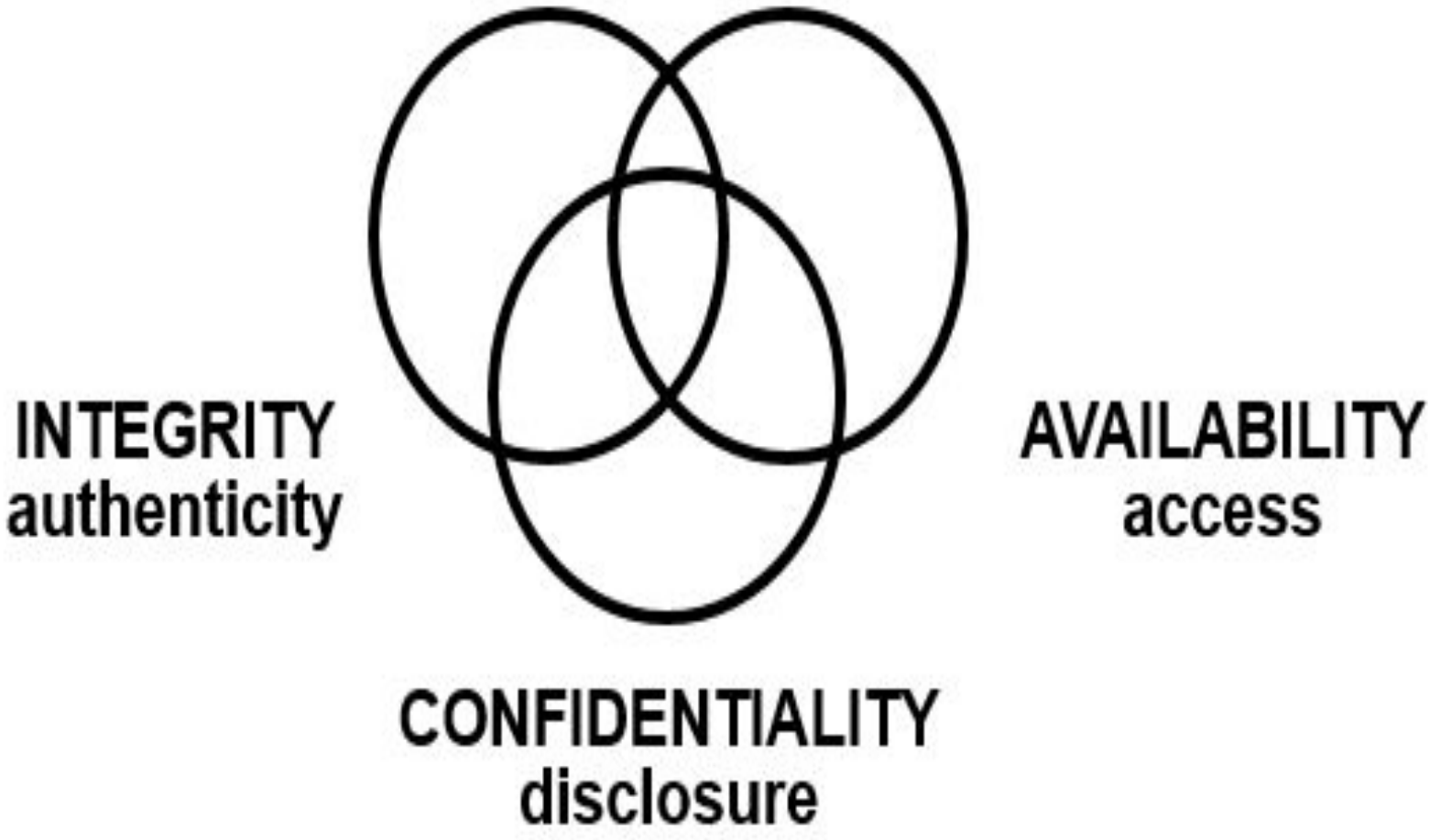
Protect Data

- Residing on Systems
- In Transit
- In Process

Control Ensure

- Authorized Access
- Acceptable level of performance
- Fault Tolerance
- Redundancy
- Reliable Backup
- Prevention of data loss or destruction

CIA TRAID


INTEGRITY
authenticity
AVAILABILITY
access
CONFIDENTIALITY
disclosure

Confidentiality

- *the property that information is not made available or disclosed to unauthorized individuals, entities, or processes*

Confidentiality

- *Confidentiality* refers to protecting information from being accessed by unauthorized parties. In other words, only the people who are authorized to do so can gain access to sensitive data.
- A failure to maintain confidentiality means that someone who shouldn't have access has managed to get it, through intentional behavior or by accident. Such a failure of confidentiality, commonly known as a *breach*

Integrity

the property of safeguarding the accuracy and completeness of assets

Integrity

Integrity authenticity of information refers to ensuring the that information is not altered, and that the source of the information is genuine.

Imagine that you have a website and you sell products on that site. Now imagine that an attacker can shop on your web site and maliciously alter the prices of your products, so that they can buy anything for whatever price they choose. That would be a failure of integrity, because your information—in this case, the price of a product—has been altered and you didn't authorize this alteration

Availability

- *The property of being accessible and usable upon demand by an authorized entity*

Availability

- *Availability* means that information is accessible by authorized users.
- Information and other critical assets are accessible to customers and the business when needed. Note, information is unavailable not only when it is lost or destroyed, but also when access to the information is denied or delayed

	Threats	Consequences	Countermeasures
Integrity	•Modification of user data •Trojan horse browser •Modification of memory •Modification of message traffic in transit	•Loss of information •Compromise of machine •Vulnerabilty to all other threats	Cryptographic checksums
Confidentiality	•Eavesdropping on the Net •Theft of info from server •Theft of data from client •Info about network configuration •Info about which client talks to server	•Loss of information •Loss of privacy	Encryption, web proxies
Denial of Service	•Killing of user threads •Flooding machine with bogus requests •Filling up disk or memory •Isolating machine by DNS attacks	•Disruptive •Annoying •Prevent user from getting work done	Difficult to prevent
Authentication	•Impersonation of legitimate users •Data forgery	•Misrepresentation of user •Belief that false information is valid	Cryptographic techniques

Cybercrime

Experts. estimate that cybercrime damages will reach $6 trillion annually by 2021, making it one of the most lucrative criminal enterprises

Reason for Cyber Crime

FINANCIAL GAIN

LACK OF AWARENESS

ANONYMITY ON THE INTERNET

WEAK CYBER LAWS

POLITICAL/PERSONAL REVENGE

Need for Cyber Security

DATA PROTECTION

INFRASTRUCTURE SECURITY

MAINTAINING TRUST

PREVENT ECONOMIC LOSS

ENSURE CONTINUITY

History of Cyber Crime

1970s–1990s

Early Hacking, Phone Phreaking

1990s–2000s

Email and Web Attacks

2000s–Now

Organized Crime, Ransomware, AI-based Attacks

Cybercriminals

Classification of Cybercrimes

- Hacking
- Identity theft
- Cyber Terrorism
- Cyber Stalking
- Defamation
- Intellectual Property crime
- Violation of privacy
- Receipt of stolen property
- Publishing or transmitting obscene material
- Spamming
- Spreading virus
- Denying access to an Authorized Person
- Damaging Computers and Disrupting Networks
- Selling illegal Items Online

Global Perspective on Cyber Crimes

- Transnational Nature
- Global Syndicates
- International Organizations: Interpol, Europol
- Cyberwarfare and Cyberespionage

Cyber Laws

Covers Data Protection, IP, e-signatures

Penalties: Fines, Imprisonment

Examples: GDPR fines, IT Act prosecutions

The Information Technology Act, 2000, was passed as the Act No.21 of 2000, got President assent on 9 June and was made effective from 17 October 2000.

The Act essentially deals with the following issues:

- Legal Recognition of Electronic Documents
- Legal Recognition of Digital Signatures
- Offenses and Contraventions
- Justice Dispensation Systems for cyber crimes

Information Technology Amendment Act 2008 was placed in the Parliament and passed without much debate, towards the end of 2008. Some of the notable features of the ITAA are as follows:

- Focussing on data privacy
- Focussing on Information Security
- Defining cyber café
- Making digital signature technology neutral
- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Recognising the role of Indian Computer Emergency Response Team
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- authorizing an Inspector to investigate cyber offences (as against the DSP earlier)

The Act totally has 13 chapters and 90 sections

Hacking and Data Theft: Sections 43 and 66 of the IT Act penalise a number of activities ranging from hacking into a computer network,

- data theft, introducing and spreading viruses through computer networks
- damaging computers or computer networks or computer programmes
- disrupting any computer or computer system or computer network
- denying an authorised person access to a computer or computer network
- damaging or destroying information residing in a computer etc.

The maximum punishment for the above offences is imprisonment of up to 3 (three) years or a fine or Rs. 5,00,000 (Rupees five lac) or both.

Receipt of stolen property: Section 66B of the IT Act prescribes punishment for

- dishonestly receiving any stolen computer resource or communication device.

The punishment for this offence under Section 66B of the IT Act is imprisonment of up to 3 (three) years or a fine of up to Rs. 1,00,000 (Rupees one lac) or both.

Identity theft : Section 66C of the IT Act prescribes punishment for identity theft

- Anyone who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person

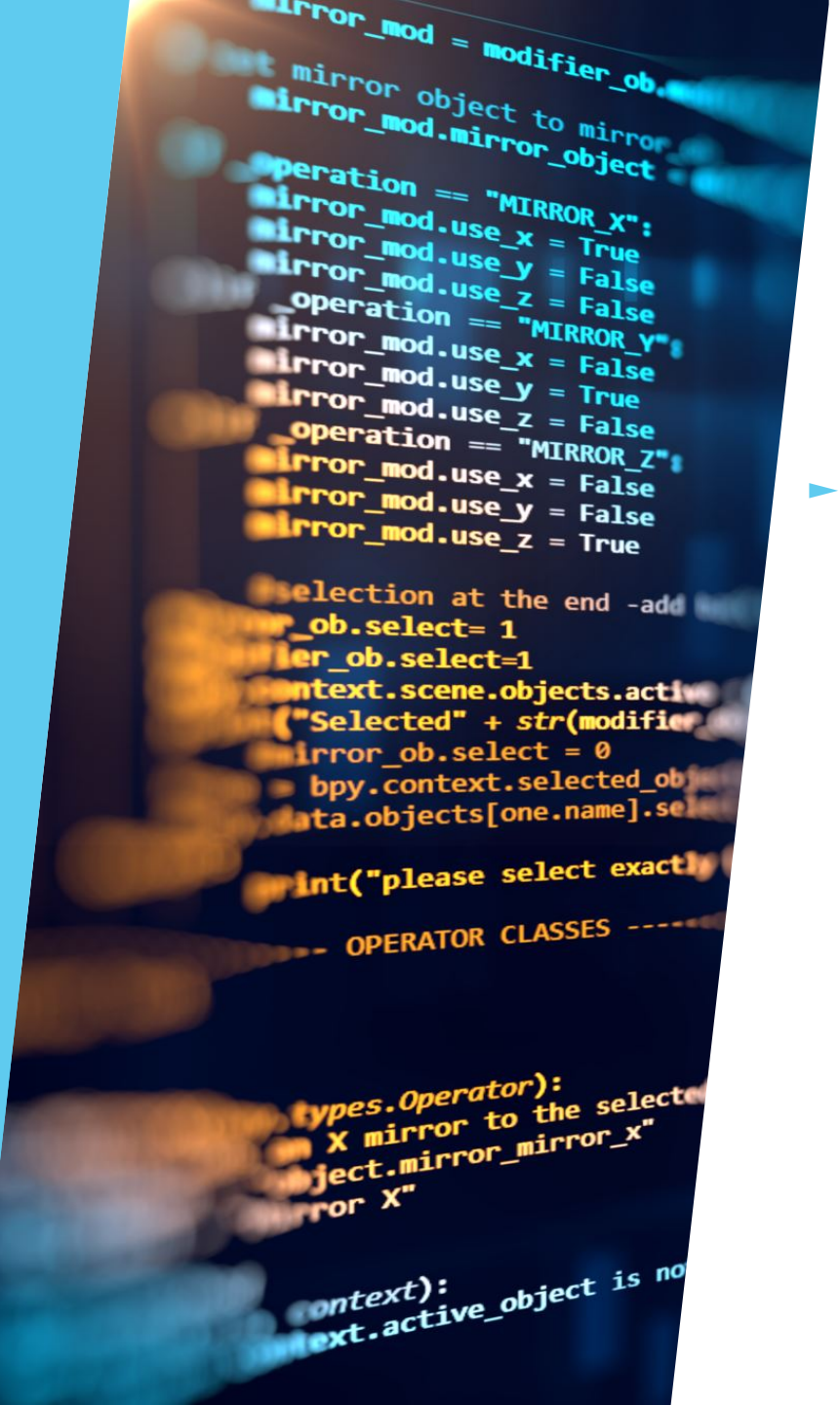
They will be punished with imprisonment of either description for a term which may extend to 3 (three) years and shall also be liable to fine which may extend to Rs. 1,00,000 (Rupees one lac).

- ***Violation of privacy:*** Section 66E of the IT Act prescribes punishment for violation of privacy and provides
- that any person who intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person,
- **shall be punished with imprisonment which may extend to 3 (three) years or with fine not exceeding Rs. 2,00,000 (Rupees two lac) or with both.**

- ***Cyber terrorism:*** Section 66F of the IT Act prescribes punishment for cyber terrorism.
- Whoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people,
- denies or causes the denial of access to any person authorized to access a computer resource, or attempts to penetrate or access a computer resource without authorisation or exceeding authorised access, or
- introduces or causes the introduction of any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect critical **information infrastructure, is guilty of 'cyber terrorism'.**

Section 69: This is an interesting section in the sense that it empowers the Government or agencies as stipulated in the Section, to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource, subject to compliance of procedure as laid down here.

The Indian IT Act, 2000



Cyber attack

- A malicious attempt, using digital technologies, to cause personal or property loss or damage, and/or steal or alter confidential personal or organizational data

Major security problems

- Virus
- Hacker
- Malware
- Trojan horses
- Password cracking

Viruses and worms

- Virus – malware attached to a carrier such as an email message or a word processing document
- A Virus is a “program that is loaded onto your computer without your knowledge and runs against your wishes
- Worm – malware can autonomously spread itself without a carrier, using information about connected computers

Solution

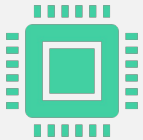
- Install a security suite that protects the computer against threats such as viruses and worms.

How To prevent hacking

- It may be impossible to prevent computer hacking, however effective security controls including strong passwords, and the use of firewalls can helps.

Malware

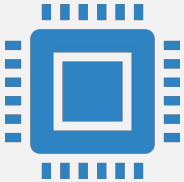
The word "malware" comes from the term "MALicious softWARE."



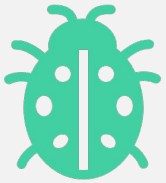
Software that has some malicious intent and which is installed on a user's computer without that user's consent.

Key loggers – Software installed on a computer that captures key strokes and sends these to a remote system. Used to try and get personal information to gain access to sites such as banks

Malware Cont.



Ransomware– Software that runs on a user's computer and demands that the user pays some other organization. If they don't, the information on their computer will be destroyed.

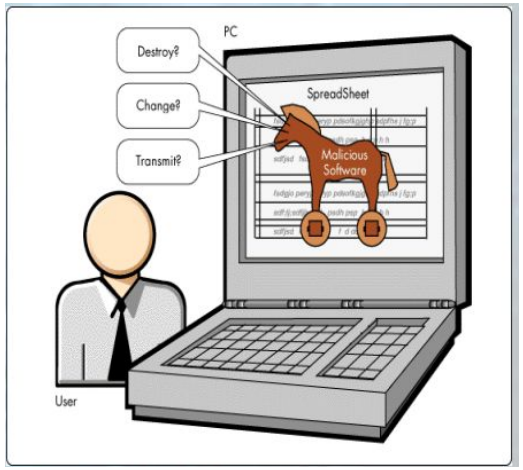


Malware can usually spread itself from one computer to another either as a virus or as a worm

To Stop Malware

- Download an anti-malware program that also helps prevent infections.
- Do not download from unknown sources
- Activate Network Threat Protection, Firewall, Antivirus.

Trojan Horses



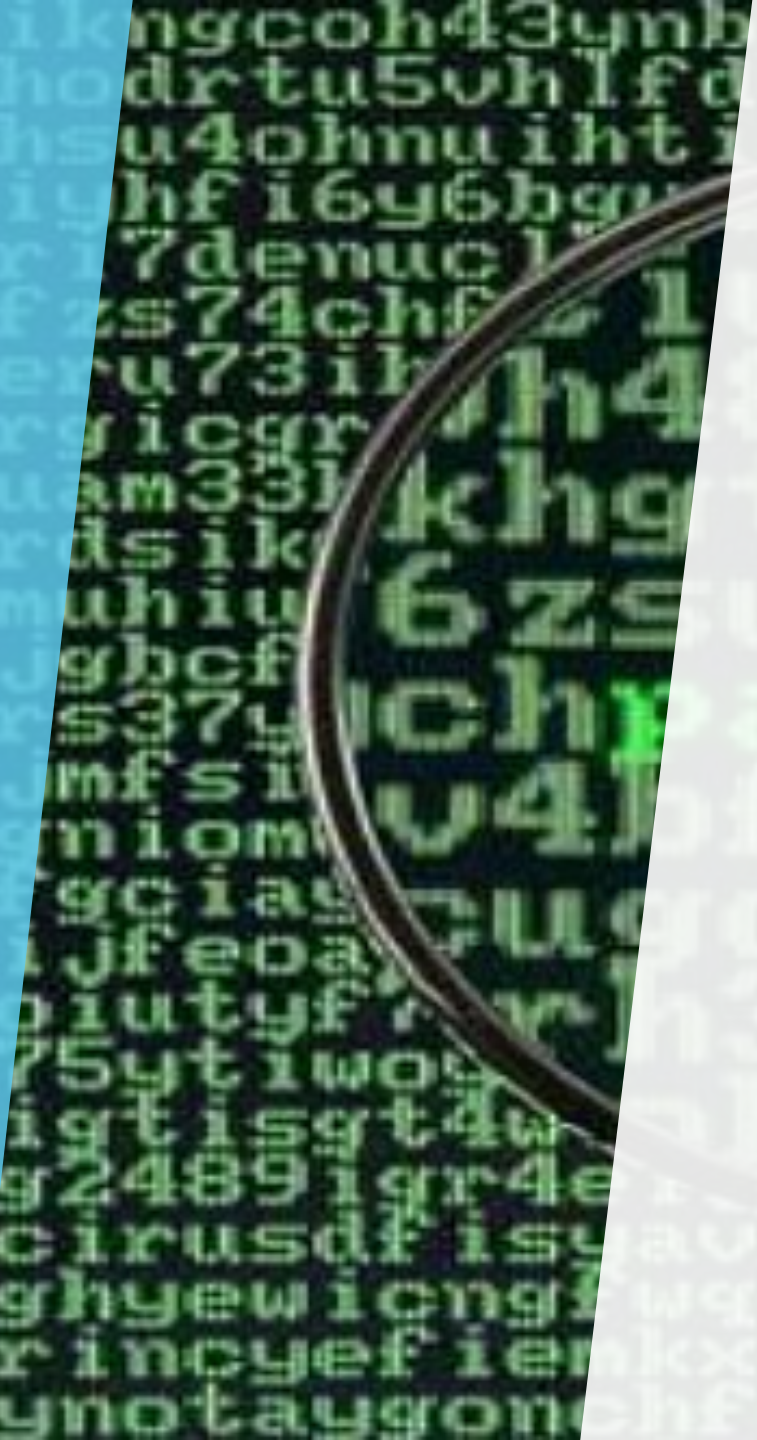
- Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system.
- These viruses are the most serious threats to computers

How to Avoid Trojans

- Security suites, such as Avast Internet Security, will prevent you from downloading Trojan Horses.
- Do not click unknown links.

Password Cracking

- Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.



Securing Password

Use always Strong password.
Never use same password for two different sites.

Insider attacks

- Attacks to an organization carried out by someone who is inside that organization either by himself or with connivance of an outsider.
- • Difficult to counter using technical methods as the insider may have valid credentials to access the system

External attacks

credentials or
of some
access to the
ns

Malicious and accidental damage

Cybersecurity is most concerned with Cyber attacks

Cyber-accidents – Accidental events that can cause loss or damage to to an individual, business or public body.

Many of the same technologies used to protect against external attack also protect against cyber-accidents.

However, sometimes protecting against cyber attacks increases the probability of cyber-accidents.

Analysis of Information Security Threats

- ***WHO***
  - *98% from external agents*
  - *4% from implicated internal employees*
  - *< 1% by Business Partners &*
  - *58% of all data thefts linked to activist groups*

Latest Trends – Information Security Threats

- **Hacktivism**
- *Hack + Activism = Hacktivism*
- *the use of legal and/or illegal digital tools in pursuit of a political / personal objective*
- *Tools and Attacks are used for*
  - *Web-site defacements*
  - *Redirects*
  - *Denial Of Service Attacks*
  - *Identity Theft*
  - *E-mail Bombing*
  - *Web-Site Mirroring*
  - *Doxing – To gather information using sourced on the internet*

Web Site Defacement

- *Web Site Defacements – Hacking and altering the website of a company's website.*

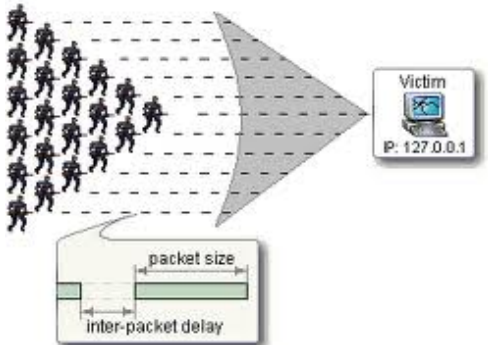
Identity Fraud / Identity Theft

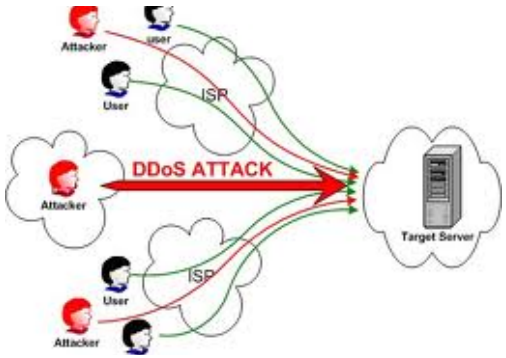
- *Stealing someone's identity in which someone pretends to be someone else by assuming that person's identity*

Doxing

- *Process of Gathering and releasing Personally Identifiable information*

Denial Of Service Attack

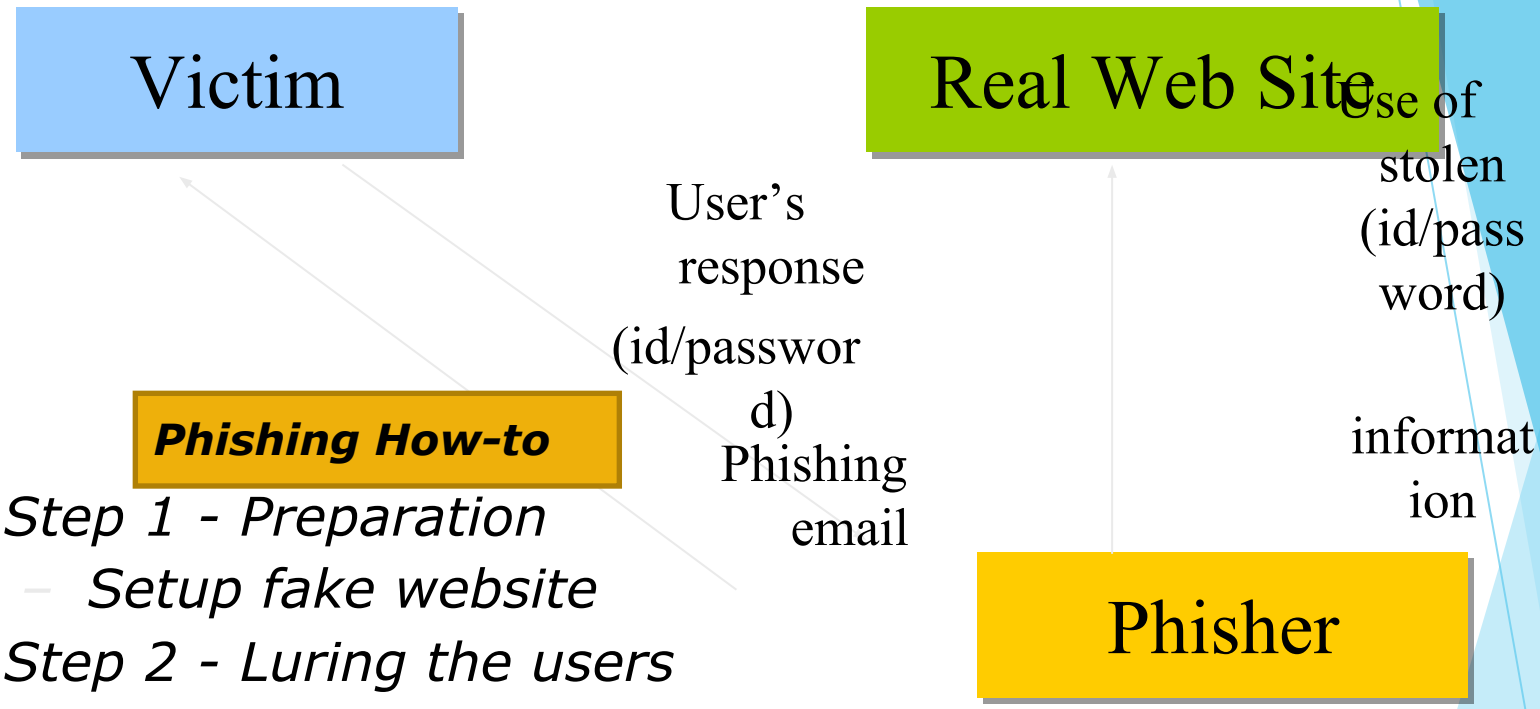




- *Attempt to make a machine or network resource unavailable to its intended users*
- *typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.*

Key Techniques Used

Key Technique Used



Phishing How-to

- *Step 1 - Preparation*
  - *Setup fake website*
- *Step 2 - Luring the users*
  - *Send Email with fake link*
- *Step 3 - Steal the details*
  - *User gives away id/password*
- *Step 4 - Use the details*
  - *Commit fraud*

Most common security mistakes

Poo

No

O

N

S

Information Security Responsibilities

	Engage Information Security teams to support the line of business, enabling secure solutions for new processes and technology
	Work with Information Security teams RISO, RISI to drive line of business-specific information security metrics reporting
	Support Regional Information Security teams in mitigating security risks from Internal Audit report findings
	Follow business continuity plans given by bank, in case of any disaster/ emergency.
	Report Security Violations and security incidents
	Adhere to Bank's Information Security Policy and guidelines
	Maintain and update Asset register of your office/dept
	Extend support to RISO during Risk Assessment and Business Impact Analysis of your office/dept



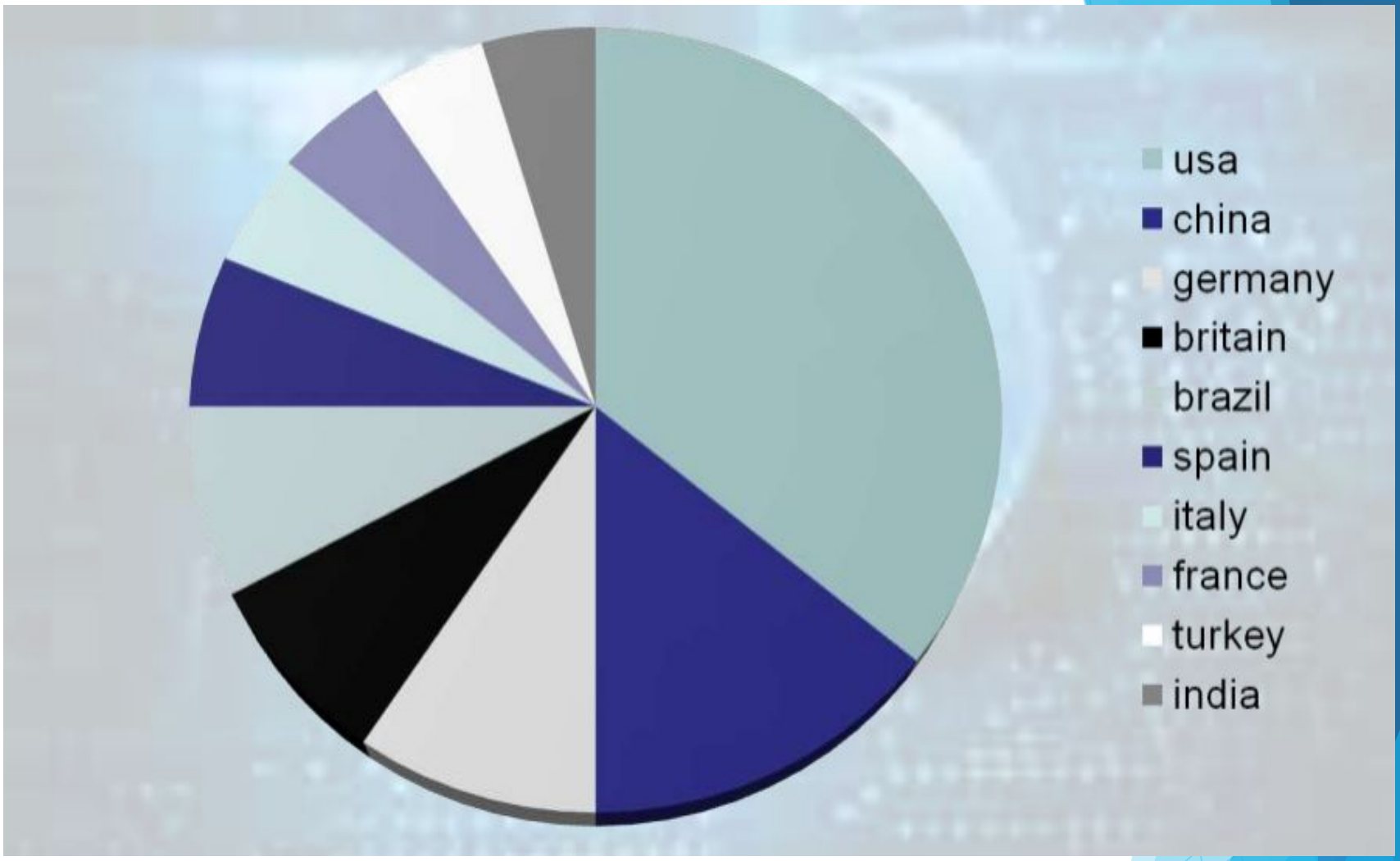



Standards & Regulations

- *ISO 27001 (Information Security Management System)*
- *ISO 22301 (Business Continuity Management System)*
- *PCI- DSS (Payment Card Industry - Data Security Standard)*
- *IT Act 2000 & ITAA 2008 (Information Technology Act, India)*
- *RBI Guidelines (Reserve Bank of India)*

Cyber Security Is Everyone's Responsibility

Robert Statica – Cybersecurity



India stands 10th in the cyber crime in the world

THANK YOU