Review & Exam Preparation session
(Modules 3 & 4 : DISSA Course)

Arijit Chakraborty

April 24, 2022

Module 3: BCP & DRP

- BCP –DRP Overview
- Key terms & concepts
- RPO, RTO
- Pre DR ICQ, BCDR Process Flow
- BC DR QRH
- BCP- Internal Audit Role – IIA Guidelines
- DRaaS : BC DR Software capabilities
- BCDR – Detailed IS Audit Checklist
- ISO 22301 – BCM

WHAT IS BUSINESS CONTINUITY:

- Business continuity : **plan to deal with difficult situations**, so organization can continue with **as little disruption** as possible.
- Whether it's a business, PSU , or charity, - BCDR is vital

Excerpt from DISSA Study Material

What is disaster recovery? A subset of BC

Disaster recovery includes the backup systems and IT contingency methods for organization's critical functions and applications.

Disaster recovery, as part of an overall BC plan, is about restoring IT systems and operations as efficiently as possible following a disaster. DR includes the backup systems and IT contingency methods for organization's critical functions and applications.

What's the difference between business continuity and disaster recovery?

The former is the overarching plans that guide operations and establish policy. Disaster recovery is what happens when an incident occurs.

Disaster recovery is the deployment of the teams and actions that are sprung. It is the net results of the work done to identify risks and remediate them. Disaster recovery is about specific incident responses, as opposed to broader planning.

After an incident, one fundamental task is to debrief and assess the response, and revising plans accordingly.

Business Impact Assessment

The impact assessment is a cataloguing process to identify the data of company holds, where it's stored, how it's collected, and how it's accessed. It determines which of those data are most critical and what the amount of downtime is that's acceptable should that data or apps be unavailable.

DISASTER RECOVERY PLANNING:

- **Disaster recovery plan (DRP)** : documented, structured approach that describes how an organization can quickly resume work after an unplanned incident.
- **DRP =** essential part of business continuity plan (BCP).
- Applied to aspects of organization that depend on functioning IT infrastructure.
- DRP : help an organization **resolve data loss & recover system functionality** so that it can perform after incident, even if it operates **at a minimal level**.

Standards Supporting BCP & DRP

- ISO 27001: Requirements for Information Security Management Systems.
- Section 14 addresses business continuity management.
- ISO 27002: Code of Practice for Business Continuity Management.
- ISO 22301 – BCMS
- RBI – BCP & DRP
- IRDAI - -do-
- SEBI - -do-
- NIST 800-34
  - Contingency Planning Guide for IT Systems.
  - 7 step process for BCP & DRP projects
  - From U.S. National Institute for Standards and Technology

- HIPAA: Requires a documented & tested disaster recovery plan
  - U.S. Health Insurance Portability and Accountability Act

BCP & DRP Differences

- **BCP**
  - Activities required to ensure **continuation of critical business processes** in an organization
  - Alternate personnel, equipment, and facilities
  - Often includes non-IT aspects of business
- **DRP**
  - **Assessment, salvage, repair, & eventual restoration** of damaged facilities and systems
  - Often **focuses on IT systems**

Business Continuity Planning vs. Disaster Recovery Planning

- Both are directed at recovery of operations
- BCP = directed at **recovery and resumption of business activities** across entire enterprise
- DRP = usually directed **at the recovery of IT systems** & Biz apps , including corporate data
- BCP addresses **Processes, People and Property**

Natural Disasters

1. **Geological:** earthquakes, volcanoes, tsunamis, landslides
2. **Meteorological:** hurricanes, tornados, wind storms, hail, ice storms, snow storms, rainstorms, & lightning
3. **Other**: avalanches, fires, floods, meteors - meteorites, & solar storms
4. **Health:** widespread illnesses, quarantines, pandemics

Not all disruptions are disasters

Man-made Disasters

1. **Labor:** strikes, walkouts, & slow-downs that disrupt services and supplies
2. **Social**-political: war, terrorism, sabotage, vandalism, civil unrest, protests, demonstrations, cyber attacks, & blockades
3. **Materials**: fires, hazardous materials spills
4. **Utilities**: power failures, communications outages, water supply shortages, fuel shortages, and radioactive fallout from power plant accidents

STEPS OF BCP & DRP:

- **1. Define Key Assets & Operations**
  (BC/DR) efforts start with identification of key assets of infrastructure & processes - important to keeping business operational.
- **2. Determine Downtime, Availability, & Recovery Window**
  Time is money.
- Determine value of investment used to strengthen BC/DR Plan.
- **3. Define Recovery Solutions**
  Define appropriate approach & solutions based on defined assets & recovery window.

4. Draft a Plan

BC/DR plan : Key processes, communication SOP & assigned responsibilities

5. Establish a Communications Plan & Assign Roles

Establish communication plan & assign roles to key members of BC/DR team.

6. Disaster Recovery Site Planning

decide on systems or capabilities required to deliver BC/DR plan.

7. Accessing Data & Applications

Define communications & security protocols for accessing data & apps.

8. Update the BC/DR Plan, In Detail

Develop detailed plan for each system & review what needs to be in place **to implement failover to secondary/redundant connections & offsite storage.**

9. Test , Refine & Audit BC/DR Plan

Organize & execute according to each system's plan.

Step D : Develop Key Recovery Targets

- **Recovery time objective (RTO)**
  - Period of time from disaster onset to resumption of business process
  - Based on acceptable downtime
  - Indicates earliest point in time at which the business operations must resume after a disaster
- **Recovery point objective (RPO)**
  - Maximum period of data loss from onset of disaster counting backwards
  - Amount of work that will have to be done over

Recovery time objective (RTO) – The acceptable downtime for critical functions and components, i.e., the maximum time it should take to restore services. A different RTO should be assigned to each of business components according to their importance (e.g., ten minutes for network servers, an hour for phone systems).

Recovery point objective (RPO) – The point to which the state of operations must be restored following a disruption. In relation to backup data, this is the oldest age and level of staleness it can have. For example, network servers updated hourly should have a maximum RPO of 59 minutes to avoid data loss.

RPO – Essence

- **RPO :** time-based **measurement of maximum amount of data loss** that is tolerable to organization.
- **How far back IT must go**, stretching back in time from disaster to the last point where data is in a usable format
- How **frequently entity needs to back up** data,
- **How much data is lost** following a disaster
- RPOs measure back in time to **when data was preserved in usable format**, usually to most recent backup
- If enterprise backs up its data every 24 hours, then only risk of losing data within last 24 hours
- RPO of 60 minutes requires system backup every 60 minutes.
- **Automatic RPO strategies** used

RPO & Industry – Tier 1

- RPO measured in hours.
- **0-1 HOUR**
- If business requires **frequent monitoring & securing** of data---**Tier 1 RPO**
- used in businesses **with high data flow & many variables**.
- Eg : Bank, FI , records in hospitals or universities –

RPO – Tier 2

- **1-4 HOURS**
- available to organizations with sensitivity level **relatively lower** than RPO -1 .
- used for certain sub-sections of an organization's database

RPO – Tier 3

- **4-12 HOURS**
- used for businesses with a relatively free data set.
- **Example:**

✓ Email lists,

✓ marketing records,

✓ sales logs

RPO – Tier 4

- **13-24 HOURS**
- ➢ not as sensitive
- ➢ database of these businesses / subsets can tolerate up to 24 hours of an RPO backup.
- ➢ have less data activity when compared to the top-tier RPOs.
- **Examples** include;
- HR department,
- purchase records of a business,

RPO – Analysis

- **RPOs =** measure of disaster range & extent of recovery a database may need to undergo with respect to time frame
- **RPOs =** important in various instances of disaster & system failure.
- Eg : power outages, Ransome wares, data attacks, data corruption, user error problems etc
- RPOs = determine data size, backup frequency
- Both RTOs & RPOs **not fixed values** for all organizations.
- **Factors :**

✓ data nature,

✓ data size,

✓ company budget

RTA & RPA

- Recovery time actual (RTA) & recovery point actual (RPA) = elapsed time & lost data of an **actual recovery process** & often different from RPO & RTO.
- Only ACTUAL business disruption & disaster rehearsals **can expose** these actuals.

ISO 22301: 2019 - BCMS

ISO 22301 - 2019

- ISO 22301 specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise.
- The requirements specified are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization.
- The extent of application of these requirements depends on the organization's operating environment and complexity.
- ISO22301 applicable to all types and sizes of organizations that:
- a) implement, maintain and improve a BCMS;
- b) seek to ensure conformity with stated business continuity policy;
- c) need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption;
- d) seek to enhance their resilience through effective application of BCMS.

Standard

- A BCMS emphasizes the importance of:
- — understanding the organization's needs and the necessity for establishing business continuity policies and objectives;
- — operating and maintaining processes, capabilities and response structures for ensuring the organization will survive disruptions;
- — monitoring and reviewing the performance and effectiveness of the BCMS;
- — continual improvement based on qualitative and quantitative measures.
- **BCMS includes the following components:**
- a) a policy;
- b) competent people with defined responsibilities;
- c) management processes relating to:
- 1) policy; 2) planning;
- 3) implementation and operation;
- 4) performance assessment; 5) management review;
- 6) continual improvement;

PDCA Cycle

- **Plan-Do-Check-Act (PDCA) cycle**
- ISO 22301 ensures degree of consistency with other management systems standards, such as ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO/IEC 27001 and ISO 28000, thereby supporting consistent and integrated implementation and operation with related management systems.
- ISO 22301:2019 replaced ISO 22301:2012, which was developed based on the British standard BS 25999-2.
- Clauses 1 to 3 = set out the scope, normative references and terms and definitions
- Clauses 4 to 10 contain the requirements to be used to assess conformity to this document.

Main clauses

- — Clause 4 introduces requirements necessary to establish context of BCMS applicable to the organization, as well as needs, requirements and scope.
- — Clause 5 summarizes requirements specific to top management's role in BCMS, and how leadership articulates its expectations via a policy statement.
- — Clause 6 describes the requirements for establishing strategic objectives and guiding principles for the BCMS as a whole.
- — Clause 7 supports BCMS operations related to establishing competence & communication on a recurring/as-needed basis with interested parties, while documenting, controlling, maintaining & retaining required documentation
- — Clause 8 defines BC needs, determines how to address them and develops procedures to manage the organization during a disruption.
- — Clause 9 summarizes requirements necessary to measure BC performance, BCMS conformity, and to conduct management review.
- — Clause 10 identifies and acts on BCMS nonconformity and continual improvement through corrective action.

Types of offsite backup facilities

- •Hot sites -Fully equipped facility
- •Warm sites -Partially equipped but lacking processing power
- •Cold sites -Basic environment
- •Duplicate(redundant) information processing facility
- •Mobile sites

- **Hot sites**
- –Fully configured & ready to operate within several hours
- –Equipment & systems software must be compatible with the primary installation being backed up
- –Costs associated with use of 3rd-party hot site usually high
- –Often cost justifiable for critical applications
- –Intended for emergency operations of a limited time period & not for long-term extended use

- **Warm Sites**
- –Partially configured
- –With network connections & selected peripheral equipment, = disk drives, tape drives & controllers, but without main computer
- •**Cold Sites**
- –Basic environment to operate IPF
- –Ready to receive equipment but does not offer any components at site in advance of the need

5 levels of testing

- –Document review
- –Walkthrough
- –Simulation
- –Parallel test
- –Cutover test

1. Document Review

- Review of recovery, operations, resumption plans and procedures
- Performed by individuals
- Provide feedback to document owners
- **2. Walkthrough**
- Performed by teams
- GD of recovery, operations, resumption plans and procedures
- Brainstorming & discussion brings out new issues, ideas
- Provide feedback to document owners
- **3. Simulation**
- Walkthrough of recovery, operations, resumption plans and procedures in a **scripted "case study" or "scenario"**
- Performed by teams
- Places participants in a **mental disaster setting** that helps them **discern real issues more easily**

4. Parallel Test

- Full or partial workload is applied to recovery systems
- Performed by teams
- Tests **actual system readiness** & accuracy of procedures
- **Production systems continue to operate** and support actual business processes
- **5. Cut over Test**
- Production systems are shut down or disconnected; **recovery systems assume full actual workload**
- Risk of interrupting real business
- Gives confidence in DR (Disaster Recovery) system if it works

Vulnerability Atlas of India (VAI) -

- VAI = comprehensive document provides existing hazard scenario for entire country
- digitized State/UT-wise hazard,
- maps with respect to earthquakes,
- winds and floods for district-wise identification of vulnerable areas
- additional digitized maps for thunderstorms, cyclone and landslides.

Purpose- VAI

- use for disaster preparedness and mitigation at policy planning & project formulation stage.
- one of its kind single point source for the various stakeholders –

✓ policy makers,

✓ administration, municipal commissioners,

✓ urban managers, engineers, architects, planners, public

- to ascertain proneness of any city/location/site to multi-hazard which includes earthquakes, wind, floods, thunderstorms, cyclones and landslides.

Module 4 : Cyber Security, Threat & Forensics

- Common Cyber Attacks
- Phishing / Social Engineering Attacks,
- DoS, DDoS, Ransomware, Internal Attacks
- Vulnerability and Threat Analysis
- Digital Forensics- Audit steps
  Common Cyber Attacks
- Deception Technology – Honeypot
- Cryptography and Steganography,
- Digital Evidence
- Ethical Hacking
- Network Communication, hardware components
- Firewall Protection, Virtual Private Networks
- Antivirus and Antimalware Software
- Transmission Control Protocol (TCP/ IP)
- Demilitarized Zones (DMZ)

WEF's view

- *Cyberattacks are one of the top 10 global risks of highest concern in the next decade, with an estimated price tag of USD90 trillion if cybersecurity efforts do not keep pace with technological change.*
- *- World Economic Forum 2020*

Understanding Cyber Crime

- ***Cyber Dependent Crimes =***
- digital system is the target as well as the means of attack.
- attacks on computer systems to disrupt IT infrastructure,
- stealing data over a network using malware (purpose of the data theft is usually to commit further crime).
- ***Cyber Enabled Crimes***
- 'Existing' crimes that have been transformed in scale or form by their use of Internet.
- Use of Internet to facilitate drug dealing, people & Arms / weapons trade/ smuggling etc

Cyber Crime

- **Computer Crime**, **E-Crime**, **Hi-Tech Crime** or **Electronic Crime**
- = where a computer is the target of a crime or is the means adopted to commit a crime.
- **Examples**
- Identity theft
- Child sexual abuse materials
- Financial theft
- Intellectual property violations
- Malware
- Malicious social engineering- Phishing
- Corporate espionage

Cyber Crime – Motivation

- Money/Greed
- Curiosity
- Revenge
- Fun
- Praise seekers
- Passtime

CYBER CRIMES

E-Mail bombing:

sending a large amount of e-mails to the victim resulting in interruption in the victims' e-mail account or mail servers.

Data diddling:

altering raw data just before it is processed by computer and then changing it back after the processing is completed.

Salami attacks:

to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. A bank employee inserts a program into bank's servers, that deducts a small amount from the account of every customer

Denial of Service:

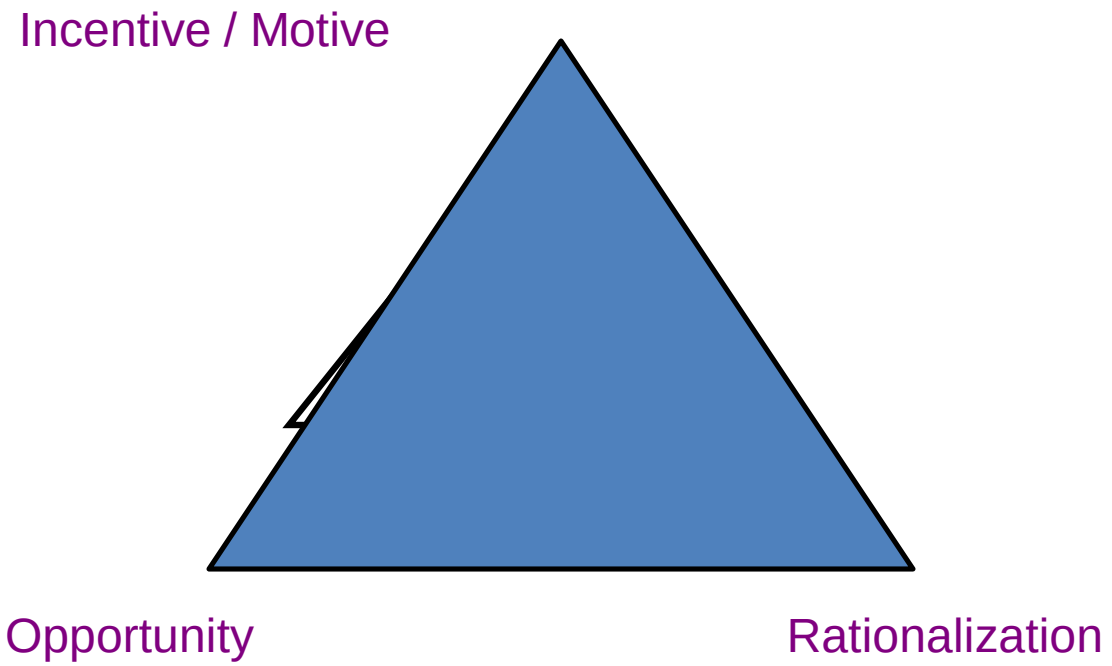
flooding computer resources with more requests than it can handle, causes resources to crash thereby denying authorized users the service offered by the resources.

CYBER CRIMES

- **Computer Based Crime-**
  - Computer used as **vehicle to commit a crime.**
  - Cyber- bullying, cyber- stalking, spamming or cyber- terrorism
- **Computer-Facilitated Crime-**
  - computer is **target of a crime.**
  - Hacking, data theft, information system is compromised.

Fraud Triangle – Psychology of Fraudster

- **Motive**
- **Rationalization**
- **Opportunity**



Hacking

- ‘Method of identifying set of vulnerabilities on target system & exploiting them systematically.
- **Ethical Hacking** = ascertains itself from hacking by adding important elements to a process - 'consent'.

1. The Process eventually **becomes a legal activity.**
2. The Ethical **Hacker seeks permission before hacking into a system** - it should be ensured hacking is **performed legally** & hacker **doesn't have any malicious intent**

Why Hacking ?

- Money extortion
- For Fun
- To Show-off
- Stealing confidential information
- To hamper privacy
- To damage System functioning
- To test security of the system

Hacking types

- **Social Engineering** - **entrapping someone with intent** to gain personal & sensitive information - User name passwords & Credit card details.
- **SQL Injection** - code injection technique for attacking data-driven applications on which malicious SQL statements are affixed to entry field to execute.
- **SQL Injections : Aim :** For **dumping complete database** of system
- For performing **various queries that are not permitted** by application
- For **changing content** of a database
- Injections = placed on search fields, address bars, and data fields.
- Make use of the " ' " characters in string

✓ **Retrieving hidden data**, modify SQL query to return additional results.

✓ **Subverting application logic**, - can change query to interfere with app's logic.

✓ **Examining database**, - extract information about version structure of database.

- **Spyware** - software with **purpose to obtain information** regarding organization or person without their assent
- **Trojan** - malicious programs **masked to be like valid programs** to make it harder for differentiating them - alter information, destroy files, or steal passwords or information

Hacking terms

- **Adware -** Software used for pushing pre-chosen ads to be displayed on system.
- **Back Door -** aka 'trap door', = hidden entry for malware - affect security measures - logins & password protections.
- **Botnet -** aka 'Zombie Army', computers controlled without knowledge of owners.
- Botnets used for sending denial or spam service attacks.
- **Brute Force Attacks -** simplest & automated kind of method for obtaining access from system or website.
- tries various combination of passwords, usernames, again & again until entry obtained
- **Denial of Service attack (DoS) -** malicious pursuit for making network resource or server unavailable for users, by disrupting or suspending services of hosted connection of Internet.
- **Logic Bomb -** Virus stashed into system provokes malicious action where few conditions are met. General version = time bomb.
- **Keystroke Logging -** tracking the keys found in computer.
- used by Black & Gray hat hackers for recording login IDs & Passwords.

Attacks

- **Malware -**
- different forms of **intrusive or hostile software** - worms, computer viruses, Trojan horses, Spyware, Ransomware, Scareware, Adware etc
- **Phishing -**
- **e-mail fraud method** -- perpetrator pushes out legitimate-looking email to obtain financial & personal information from victims
- **Spam -**
- unsolicited email aka junk mail sent to vast number of recipients
- **Spoofing -**
- used for obtaining **unauthorized access to computers** -intruder forwards message to computer with IP address , denotes that text coming from trusted host.

Attack Descriptions

- **Denial-of-service (DoS) –**
  - attacker sends a large number of connection or information requests to a target
  - so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
  - may result in a system crash, or merely an inability to perform ordinary functions
- **Distributed Denial-of-service (DDoS) –**
- a coordinated stream of requests is launched against a target from many locations at the same time

Attack Descriptions

- **Spoofing** - technique used to gain unauthorized access whereby = intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host
- **Man-in-the-Middle** - an attacker sniffs packets from the network, modifies them, and inserts them back into the network

LOG4J vulnerability- 2021

- Log4Shell, an internet vulnerability that affects millions of computers, involves obscure but nearly ubiquitous piece of software, Log4j.
- The software is used to record all manner of activities that go on under the hood in a wide range of computer systems.
- Log4j records events – errors and routine system operations – and communicates diagnostic messages about them to system administrators and users.
- First came to widespread attention on Dec. 10, 2021, Hackers using the vulnerability.

Mobile hacking

- **Key Features**
- Track location and sim card activity
- Check messages & calls
- View media files
- Hidden details - passwords , usernames, browser history,
- ● Control remotely
- 1. **Ultimate Phone Spy**
- Features - , sent & received messages, social media activities, browsing history, etc.
- inbuilt GPS tracker implanted - even track location of targeted device

Cyber incidents

- **Gaming industry**
- 152 million web application attacks & billions of incidents of credential stuffing over a 2-year period.
- Gaming industry suffered 12 billion cyberattacks between Nov 2017 - March 2019

Online gaming – IT Risks

- risks from social interactions with strangers who may trick user into revealing personal or financial information
- risks from computer intruders exploiting security vulnerabilities
- risks from online and real-world predators
- risks from viruses, Trojan horses, computer worms, and spyware

- **Black Hat Hackers**
- Crackers who perform **hacking activity with intent of obtaining unauthorized access** to system & causing a threat to its operation for stealing confidential information.
- Black Hat Hackers = always **considered illegal** because of malicious intent.
- **invade into system or network** for stealing info or money.
- Can send Spam emails by using victim's server to any email address
- Black Hat Hacker = person behind computer **who aims to find vulnerability in networks or computer** & break into it.

Grey Hat Hackers

- Hackers who have blend of **both White and Black hat hackers**.
- usually **surf into internet for looking at vulnerable threats** in System, Networks, Phone system, or Computers.
- Once they identify vulnerability, **then they hack into them & fix it.**
- Later they inform System Administrator what they do & charge a small fee for identifying the threat & fixing it.
- **Spy Hackers**
- recruited mostly in corporations for infiltrating business secrets, trading, & competition.
- Spy Hackers use same tactics like hacktivist **– but : motto of these hackers** = meet goal of client & complete assigned task.

Trojan Horse

- **Software may appear legit might be trojan**.
- A PDF / Avi contain trojan.
- Trojan horses runs in background process,
- collect information & send it to hacker.
- Trojan horses can be sent via- pen drive, ipod, website or email.
-

Password Hacking

- passwords for databases, emails, bank accounts, computer systems, servers.
- **Strong password :**
- Consists of 8 Characters
- Mix of numbers, special characters, letters
- Combination of capital & small letters.

Password hacking techniques

- **Dictionary Attack**
- hacker uses **predefined set of words from dictionary** for **guessing** passwords. When **passwords are weak**, easy for dictionary attack to decode them fast
- **Hybrid Dictionary Attack**
- makes use of **group of dictionary words** combined with **extensions.**
- Ex: word "admin" joins itself with extensions like "admin15" & " admin157",
- **Brute - Force Attack**
- hacker shall make use of **all possible sequences of special characters, numbers, numbers, small & capital letters for breaking passwords**.
- has **highest probability** of success,

Password Grabbing

- Gmail hacker / attacker target a **particular low quality** website where victim is member & **hack their database** to get stored username & password of victim.
- Many victims **use same password** for Gmail & other purposes , eg xyzsuper.com
- Easy for Gmail hacker to get victim's password through low quality website xyzsuper.com

Ethical hacking

- **Network Hacking** -
- process of obtaining **information of any Network using tools** (Ping, Tracert, NS Lookup, NetStat & Telnet). Networking hacking - performed with **intent to cause a threat to Network system** & hinder operations of network.
- **Website Hacking** -
- act of **getting unauthorized control over Web Server** & related to software like interfaces & databases. -
- GST N , Ecommerce etc
- **Email Hacking** - obtaining **unauthorized access** to Email account & executed without any consent of owner.
- **Password Hacking** - method of **mending secret passwords** from data transmitted by computer system.
- **Computer Hacking** - act of **stealing Computer ID & Password** using hacking methods & gaining unauthorized access to computer system.

Hacking

- **Uses:**
- For recovering **lost information**
- For **executing penetration testing** to intensify network & computer security.
- **Downsides :**

✓ Immense Security Breach.

✓ Hindrances in System operations.

✓ Malicious threats to system.

✓ Unauthorized access to system or private information.

White Hat Hackers (WHH)

- perform Hacking activities **with good intent**.
- **WHH : Computer Security Experts -** specialists in pen testing
- professionals who constantly defend growing technology to fight criminally-minded hackers.
- **Elite Hackers (EH)**
- Masters of all types of Hacking.
- EH – have good reputation
- EH : treated as Senior-level hackers in hacking community.
- Called ***Masters of Hacking & deception.***

Defending from cyber-threat
Internet Security

1. Access site which uses **https** (Hyper Text Transfer Protocol Secure) **-** performing Online transactions, Downloads etc,
2. If site **uses SSL/ TLS ,** verify Certificate details **-** Who is owner, Expiry date of certificate etc to confirm whether it is trusted
3. By clicking **lock icon.**
4. Scan downloaded files with **updated Anti-Virus Software** before using it.
5. Install & properly **configure a Software firewall**, to protect against malicious traffic.

Data security

1. Enable **Auto-updates of OS** & update it regularly.
2. Download **Anti-Virus Software** from Trusted Website & Install.
3. Ensure automatically **gets updated** with latest signatures.
4. Download **Anti-Spyware Software** from Trusted Website & Install, update

- **Browser Security:**

1. Always update Web Browser with latest patches.
2. Use privacy or security settings which are inbuilt in browser.

Email security

- Use **strong password** for email account.
- Always use **Anti-Spyware & anti-virus Software** to scan emails for Spam.
- Remember to **empty Spam folder.**

Firewall

- Firewall = **software or hardware device** - examines data from several networks & either permits it or blocks it to communicate with user network
- Governed by predefined security guidelines. Defends from internal & external threats
- Supervises flow of traffic between distinctive parts of network.
- Firewall always exists between private network & Internet - filters packets coming in & out.

- **2FA**
- Google account settings & enable 2FA feature.
- Google Authenticator app to ensure no one else can access account without permission.

Zero Trust principle- Security Framework : 2021

- **“trust but verify” - Traditional security framework**
- Model became obsolete with cloud migration of business transformation initiatives & acceleration of a distributed work environment due to pandemic.
- Requiring all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

CAPTCHA

- CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) = type of security measure = **challenge-response authentication.**
- CAPTCHA helps protect from spam and password decryption by asking you to complete a simple test that proves you are human and not a computer trying to break into a password protected account.

Deception technology: Honeypot

- network-attached system **set up as decoy to lure cyber attackers & detect, deflect , study hacking attempts**
- security mechanism = virtual trap to lure attackers

CERT-In Guidelines on Cyber-Security Audit

- Auditee and Auditing organizations needs to re-assess their risk profile and implement controls for minimizing the risk.
- Architecture changes, exposure of services, expanded organizational boundaries and changes caused = to be reviewed by Cyber Auditor
- Services exposed on adhoc and temporary basis (Pandemic) needs to be secured and properly audited. Such temporary changes to be reflected in BCP of organizations and thoroughly tested by Cyber / Forensic Auditor.
- Auditor & auditee organisation = ensure quality of audits should not be lowered in case of remote assessment = use of techniques : video calling for evidence verification, asking for snapshot of command output, online interview of process owner / suspect / witness etc
- Auditor = to maintain situational awareness & their assessments should also include tests derived from recent cyber-attacks trends

- Auditor to develop SOP for each type of audits and be clearly communicated to employees and auditee organization
- Periodic cybersecurity audits and audits when there is change in apps or infrastructure are critical & should not be avoided /diluted
- **Focus on ‘’External ‘’ audit**

❑ Internal as well as external third-party audits are recommended for the cyber infrastructure of the organizations.

❑ To ensure independence and audits by domain experts, external audits should not be replaced by internal audits only.

- **SOP for Cyber / Forensic Audit engagement team**

- Employees deployed for audit should connect to centralized server of auditing firm and all audits related activity should only be conducted by connecting to the office network
- Auditors should only use office provided devices for conducting audits and these devices should only be used exclusively for audit activities.
- Auditing firms must follow CERT-In **Secure Data handling Guidelines**
- **Audit evidence / Data** should only reside at auditing Firm's servers at centralized location, NOT in auditee organisation server

Control gaps review & Audit Report

- Generate all security testing reports and recommendations.
- Suggest best possible patching and remediation for the identified vulnerabilities.
- Discuss & document the management action plan with timeline to implement the recommendations on the same
- In collaboration with client IT staff, resolve all the gaps identified in VAPT , and re-assess the vulnerability post closure of gaps
- Cyber security auditor = to submit recommendation, final audit report after the remedies/recommendations are implemented.
- The final report will certify the particular - Website “Certified for Security”.

Types of Network Topologies

- *#1)* ***BUS Topology:***
- Every network device connected to single cable & transmits data **only in 1 direction.**
- **Advantages:**
- Cost-effective
- Can be used in small networks.
- Very less cable is required when compared to other topologies.
- **Disadvantages:**
- If cable gets faulty then the whole network will fail.
- Slow in operation.
- Cable has limited length.

- ***RING Topology:***
- Each computer connected to another computer in the form of a ring with last computer connected to first one.
- Each device - 2 neighbors. data flow is unidirectional & bidirectional
- **Advantages:**
- Easy to install and expand.
- Can be easily used for transmitting huge traffic data
- **Disadvantages:**
- Failure of one node will affect the whole network.
- Troubleshooting is difficult in a ring topology.

- ***STAR Topology:***
- All nodes are connected to a single network device through a cable.
- **Advantages:**
- If one node fails, then it **will not affect the whole network** and the network will run smoothly.
- Troubleshooting of fault is easy.
- Simple to operate.
- **Disadvantages:**
- High cost.
- If central node gets faulty = whole network will get interrupted

- ***MESH Topology:***
- Every node **connected to another one with a point to point topology** & **every node connected to each other.**
- **Advantages**:
- It is robust.
- Fault can easily be detected.
- Very secure
- **Disadvantages**:
- Very costly for Installation & configuration

TCP IP

- IP = how **to address & route each packet to make sure it reaches right destination**.
- Each gateway computer on network checks this IP address to determine where to forward the message.
- **Uses of TCP/IP**
- used to provide remote login over network, for:

✓ interactive file transfer,

✓ to deliver email,

✓ to deliver webpages over the network

Common TCP/IP protocols

- **HTTP (Hypertext Transfer Protocol)**, = communication between web server and web browser;
- **HTTPS (HTTP Secure)**, = secure communication between a web server and a web browser;
- **FTP (File Transfer Protocol)**, = transmission of files between computers.

Types of Transmission Media

- ***1. Coaxial Cable:***

= 2 conductors which are parallel to each other. Copper used as a central conductor & surrounded by PVC installation with outer metallic wrapping.

- **Cable TV network** providers also widely use **Coaxial cable in entire TV network.**
- ***2.Twisted Pair Cable***
- **Most popular** wired transmission medium. Cheap & easier to install than coaxial cables.
- 2 conductors (copper), each having their **own plastic insulation & twisted with each other**. One is grounded & other **used to carry signals** from sender to receiver.
- used in LAN & telephone landline connections - has high-bandwidth capacity

3. *Fiber Optic Cable:*

- made up of a **core surrounded by a transparent cladding material**
- It uses **properties of light for signals** to travel between them.
- used in WAN
- Optic fiber = flexible & transparent fiber - consists of **silica glass** or plastic.
- Optic fibers transmit signals in form of light between 2 ends of fiber = **they permit transmission over longer distances & higher bandwidth** than coaxial & twisted pair cables or electrical cables.

Network layout & domains

- **A. Trusted Zone –**
- secure zone with restricted access.
- **Consists of –**
- storage,
- database &
- management servers = not directly accessible to outside zone.
- Trusted zone **separated using strong access** control & firewall, - additional level of security to infrastructure.

- B. De-militarized Zone – (DMZ)
- "neutral zone" between internal network & outside extranet network.
- Small network = lies between trusted internal network (LAN) & un-trusted external network (Internet).
- DMZ is isolated using security gateway (i.e., firewall) to filter traffic between DMZ & private network.
- DMZ itself has security gateway in front to filter incoming traffic
- DMZ contains devices accessible to Internet traffic, such as Web, FTP, SMTP & DNS servers
- Goal of DMZ = allow access to resources from untrusted networks while keeping private network secured
- DMZ server = resides in DMZ & used to externalize resources to public network

IDS and IPS

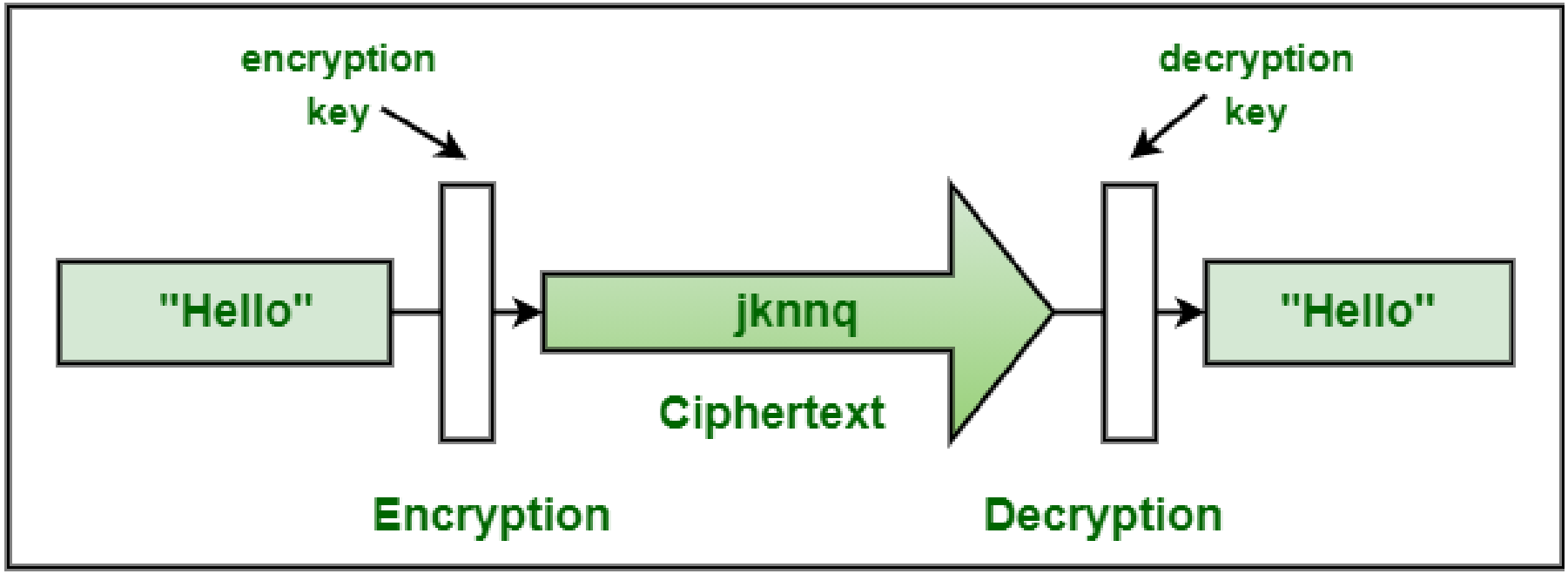
- Intrusion detection is the process of monitoring the events occurring in network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies.
- Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents.
- These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which become part of network to detect and stop potential incidents.

CYBER FORENSIC

- **Digital Forensic**
- *"Process of identifying, preserving, analyzing and presenting digital evidence in a manner that is legally acceptable in any legal proceedings (i.e., a court of law)."*
- **Digital Evidence** =
- any information, data of probative value stored in binary form, transmitted , received by an electronic devices.

Cryptography

- Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents.
- The term is derived from Greek word *kryptos,* means: hidden.
- The National Institute of Standards and Technology (NIST) started development of AES in 1997 when it announced the need for an alternative to the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks.
- AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages.
- AES-192 uses a 192-bit key length to encrypt and decrypt a block of messages.
- AES-256 uses a 256-bit key length to encrypt and decrypt a block of messages



Cryptography

256 Bit Encryption

- A 256-bit encryption key is significantly more difficult for brute-force attacks to guess than a 128-bit key;
- however, because the latter takes so long to guess, even with a huge amount of computing power, it is unlikely to be an issue for the foreseeable future

Steganography

- Steganography, the practice of hiding information, has been around for centuries.
- Digital steganography usually involves hiding data inside innocuous files such as images, videos, and audio
- Malicious hackers use steganography for a variety of tasks such as hiding malicious payloads and script files.
- Malware developers often use LSB steganography to hide the code for their malware in images of celebrities and famous songs and execute them with another program after the file is downloaded on the victim's computer.

LSB Algo

- One of the most popular techniques is 'least significant bit (LSB) steganography. In this type of steganography, the information hider embeds the secret information in the least significant bits of a media file.
- For instance, in an image file each pixel is comprised of three bytes of data corresponding to the colors red, green, and blue
- LSB steganography changes the last bit of each of those bytes to hide one bit of data.
- To hide one megabyte of data using this method, we need an eight-megabyte image file.
- Since modifying the last bit of the pixel value doesn't result in a visually perceptible change to the picture, a person viewing the original and the steganographically modified images won't be able to tell the difference.

Differences between steganography and cryptography

- While steganography hides information, cryptography focuses on rendering the data unreadable to everyone except its intended recipient.
- Once a stream of data is encrypted, only a person who has access to its decryption key will be able to unlock it.
- The practice of detecting steganography is called 'steganalysis'.
- There are several tools that can detect the presence of hidden data such as StegExpose and StegAlyze