Chapter 12 - "Digital Auditing and Assurance"

(B) Advanced Topics:

(i) CYBER Risk:

(a) Meaning and Types of Cyber Risk:

↓

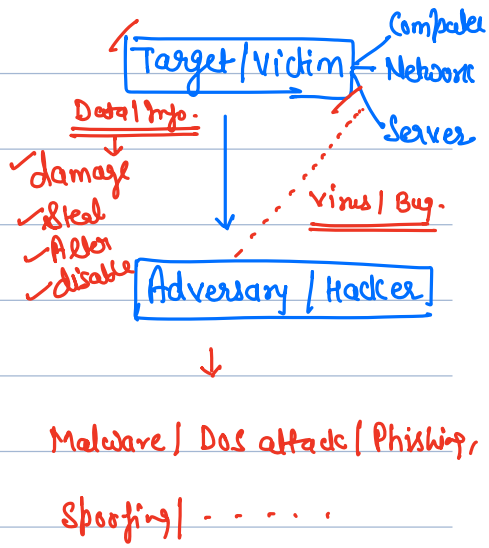
- Risk of damage, steal, Alter, disable or destroy of data due to cyber-attack.

↓

Attempt to gain unauthorised access to a computer system, network or server.

↓

with an intent to cause damage, steal, alter, disable or destruct the data.



Malware / DoS attack / Phishing, Spoofing / - - - -

Types of Cyber-Risk:

(a) **Malware:** Programs that are created with intent to do harm to a computer system, network or server.

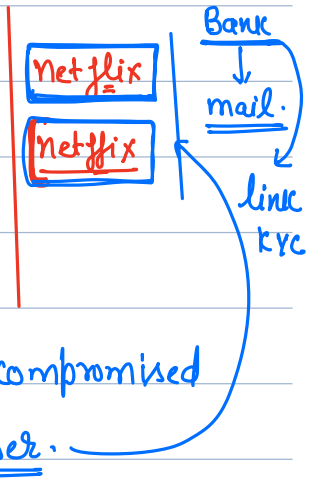
Ex: Ransomware, Fileless Malware, Trojan, Mobile Malware.

(b) **DoS Attack:** Targeted attack that floods a network with false requests - (Denial of Service) to disrupt the business operations.

Users are not able to perform routine tasks like assessing e-mails, website or other resources operated by compromised system.

(c) **Phishing**: Use of e-mails, SMS, Phone, social media etc. to entice a victim to share sensitive information such as OTP, Passwords, Account number, CVV etc.

(d) **Spoofing**: Accessing systems or devices of target using **fake identity**, with ultimate goal of stealing information, extorting money, installing malware, etc.



(e) **Identity Based attacks**: Valid User's Credentials have been compromised and an adversary is pretend to be that user.

(f) **Insider Threats**: Employees (former or current) having direct access to company network, sensitive data, polices and other information.

(b) **Stages of Cyber Risk**:

Assessing CYBER Risk → **Evaluate the Impact of CYBER Risk** → **Managing CYBER Risk**

Consider threats like:
(a) Ransomware
(b) E-mail Phishing
(c) Insiders Committing malicious activities

Evaluate the Impact of CYBER Risk w.r.t.
(a) Regulatory cost
(b) Business interruptions
(c) Data loss
(d) Reputation loss and litigation
(e) IP Theft
(f) Incident Response cost
(g) Breach of Privacy
(h) Fines and Penalties
(i) Ransomware

Managing CYBER Risk
(a) Gain a holistic understanding of Cyber Risk.
(b) Assess existing IT and cyber security programs.
(c) Align cyber security initiatives with strategic objectives.
(d) Understand accepted risk.
(e) Document compensating controls.

(c) Cyber Security Framework : (CSF) — Identify
Protect
Detect
Respond
Recover

IPDR$_2$

Cyber Security framework includes the following activities:

(1) Identify the Risk: through (i) Risk Assessment
(ii) Asset Management
(iii) Governance structure
(iv) Economic / Business Environment

(2) Protect the Risk: through (i) controlling unauthorised access.
(ii) formal training
(iii) Controls for data security.

(3) Detect the Risk: through the adequate controls, Policies and procedures.

(4) Respond to the Risk: Includes (a) Response Planning
(b) Communication
(c) Mitigation Process

(5) Recovery from Risk: includes (a) Recovery Plans
(b) Improvements e.g. Antivirus; Patch upgrades etc.

(D) Control Considerations - Cyber Risk :

(i) Vendor set-up and Modifications

↓

Control considerations includes

↓

(a) Who is **Responsible** for changes in Vendor Master files.

(b) **Process** - Centralised or - Decentralised.

(c) **Communication Channels** used to request changes to Vendor Masters data. (e.g. Use of Multi factor authentication)

(d) **Systems and Techniques** used to Initiate, authorise and Process the requests related to changes in Vendors Master Data.

(e) Are **Authentication Protocols** defined to verify the modifications. (e.g. Call back ; Multi-factor Authentication

(ii) Electronic transfer of funds

↓

Control considerations includes

↓

(a) Are Persons engaged in the activity are aware of **threats and information** related to common Phishing Scams.

(b) Are **authentication Protocols** defined to verify the transfer requests. (e.g. Call back ; Multifactor authentication)

(c) **System and Techniques** used to initiate, authorise and facilitating the request including release of transfer money.

(iii) Patch Management

↓

Control consideration includes

↓

(a) **Existence** of Patch Mngt. System.

(b) **Periodic scanning** to identify missing patches.

(c) How **entity notified** of Patches by External Vendors.

Imp:

(E) Remote Audit : - to be covered from book -

Meaning : Using online or electronic means to Conduct the audit.

Note: Audit Evidences are obtained or documentation review is done with participation of auditee.

Considerations: (A) Planning and Feasibility:

involves agreeing on - audit timelines; - meeting platform - data exchange mechanism - access authorisation requests.	Ensure feasibility of use of technology ↓ based on competence and resources of auditor and auditee.

(B) Confidentiality, Security and Data Protection:

- Ensure restricted access to document sharing platform
- Ensure timely removal of information from platform, subsequent to review and documentation by auditor.
- Consider applicable legislation and regulations.
- Use of VPN for accessing auditee IT System.

(C) Risk Assessment:

- Risk of achieving audit objectives - identified, assessed and documented.
- Assess whether remote audit would be sufficient to achieve audit objectives.

Advantages and Disadvantages: (Noting - H.W.)

(ii) Emerging Technologies in Audit:

✓ DATA ANALYTICS:

✓ Generating and Preparing meaningful information from raw system data using processes, tools and Techniques is known as Data Analytics.

Tools / Techniques
↓
Raw Data
↓ Process
meaningful info
↓
insights, trend, patterns
↓
to identify any irregularities / fraud.

✓ Data Analytics analyses large set of data to find actionable insights, trends, patterns, draw conclusion and informed decisions.

✓ Data Analytics enables greater efficiencies and more accurate findings.

✓ Data Analytics helps the auditor to audit ① more effectively and ② large amount of data held and processed in IT System.
It also benefits the auditor in discovering and analysing trends, identifying anomalies and extracting useful information from data.

✓ Data Analytic Methods used in an audit are known as Computer Assisted Audit Techniques (CAATs).

Examples of CAATs:

(A) Audit Command Language (ACL): - Software used for fraud detection and prevention
- ACL samples large set of data to find patterns that indicate fraud / control deficiencies.

(B) Alteryx : used for consolidation of financial or operational data to assess controls.

(C) Power Bi : It is a Business Intelligence Platform that provide, non-technical business users, with the tools for aggregating, analying, visualising and sharing data.

(d) CaseWare : Data Analysis Software that provide tools for Conducting audit - quickly, accurately and consistently.

Imp.

Examples of tests that can be performed with CAATs : (from book)

(1) Identify Exceptions
(2) Identify Errors
(3) Verify Calculations
(4) Existence of Records
(5) Data Completeness
(6) Data consistency
(7) Duplicate payments
(8) Accounts exceeding authorised limit.