SUB: Cyber Security

Unit 6 : Cybersecurity Organizational Implications

Prof: Morade D.S.

6.1 Organizational Implications: Cost of Cybercrimes and IPR Issues

- Because the internet is always connected worldwide, there is always a chance of cyber-attacks (hackers, viruses, malware, web attacks).
- When cybercrimes happen, organizations lose a lot of money.
- These losses can be due to **malicious code, viruses, and web attacks** that break through the company's firewall (security system).
- That's why companies are very worried about the **high cost of cybercrimes**.

6.1.1 Internal Cost of Cyber Security Incidents

When a cyber-attack happens, a company not only loses money directly but also has **internal costs**. These include:

1. **People Cost**
   - Money spent on employees who investigate, repair, or prevent cyber-attacks.
   - Example: Hiring IT experts, cybersecurity teams, or paying overtime to fix the problem.
2. **Overhead Cost**
   - Extra expenses that come because of the incident.
   - Example: Buying new security software, upgrading firewalls, or paying for legal advice.
3. **Productivity Losses**
   - When systems are down or attacked, employees cannot work properly.
   - Example: If the company's website is hacked, customers cannot place orders → company loses business, employees sit idle.

 Simple Example:
Imagine a shopping website (like Amazon).

- If hackers attack it, the company must pay experts to fix the issue (**people cost**).
- They might need to buy better security software (**overhead cost**).
- Meanwhile, customers cannot buy products during the downtime, and employees cannot process orders (**productivity loss**).

The money a company loses in a cyber-attack depends on:

- **Attack type** (virus, malware, phishing, etc.)
- **Industry type** (banking, defense, healthcare, etc.)
- **Company size** (big companies lose more money compared to small ones).

 Example: A bank (financial sector) is more likely to be attacked than a small shop, because banks deal with money and sensitive customer data.

When a cyber-attack happens, companies spend money in different areas:

- **Direction cost (25%)** → Money spent by management to take big decisions during/after attack.
- **Recovery cost (21%)** → Fixing damaged systems, restoring data, getting back to normal.
- **Post-response cost (19%)** → Expenses after the attack (monitoring, legal support, extra training).
- **Investigation cost (14%)** → Finding out how the attack happened and who did it.
- **Escalation & incident management cost (12%)** → Handling the crisis properly, involving higher authorities.
- **Containment cost (9%)** → Stopping the attack from spreading further.

 Example: If a company website is hacked, they spend money on IT experts to investigate, lawyers to handle legal issues, and management meetings to control the situation.

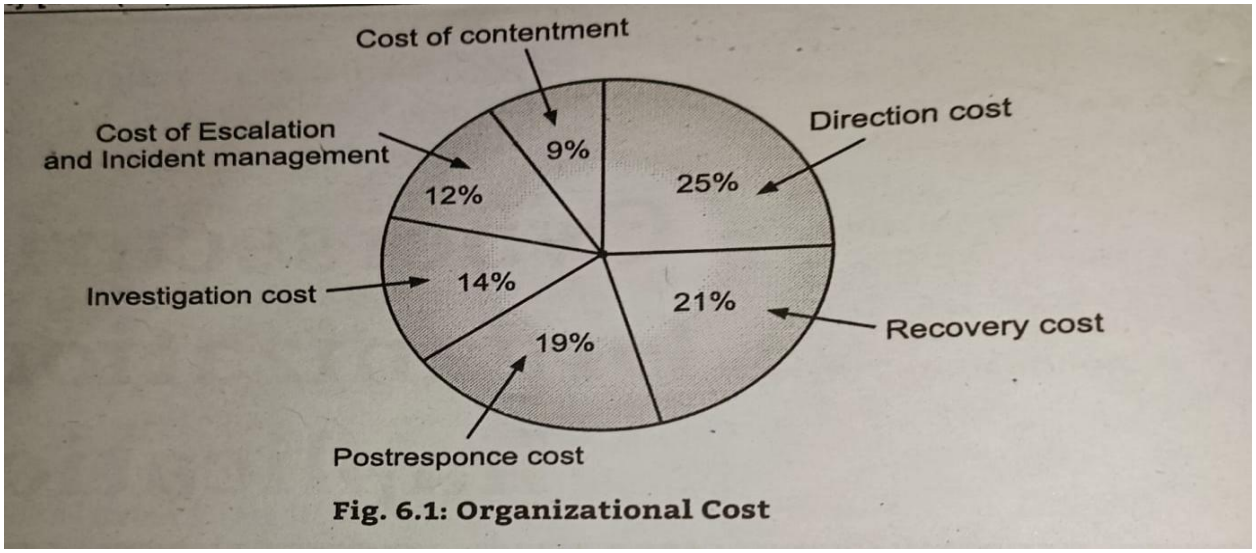

Fig. 6.1: Organizational Cost

Consequences of Cybercrime

The results of a cyber-attack and their costs:

- **Information/data loss (42%)** → Losing confidential customer or company data.
- **Business disruption (22%)** → Systems go down, work stops.
- **Loss of revenue & brand damage (13%)** → Customers lose trust and company loses sales.
- **Damage to equipment (13%)** → Hardware or software may be broken.
- **Other costs (10%)** → Extra miscellaneous costs.

 Example: If hackers steal customer credit card data from an online store, the company not only loses data (42%), but also loses customers because people no longer trust the store (brand damage).

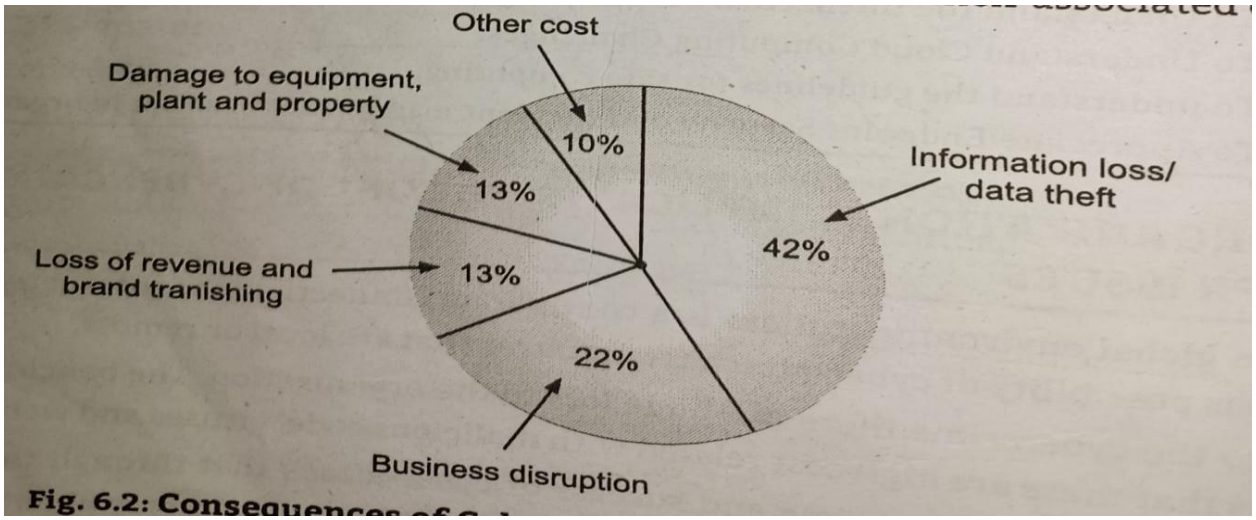

Fig. 6.2: Consequences of C...

Common Cyber Attacks

According to studies:

- **Viruses, Worms, Trojans** → 100% organizations affected
- **Malwares** → 80%
- **Botnets** → 73%
- **Web-based attacks** → 53%
- **Phishing & social engineering** → 47%
- **Stolen devices** → 36%
- **Malicious insiders** → 29%
- **Malicious code** → 27%

 Example: If an employee's laptop is stolen (36%), hackers may use it to steal company data.

How to Protect Data (Preventive Measures)

1. **Endpoint Protection**
   - Endpoints = devices connected to a network (like printers, laptops, mobiles).
   - These are often ignored but can be hacked.
     Example: A hacker enters the company network through an unsecured office printer.
2. **Secure Coding**
   - Developers should write software in a safe way so hackers cannot insert malicious code.
     Example: A banking app is built with strong coding practices so that hackers cannot easily steal login details.
3. **HR Checks**
   - Check employees' background before hiring, and monitor their activities even after hiring.
     Example: If an employee has a history of data theft in past jobs, the company can avoid hiring them.
4. **Access Controls**
   - Give permissions carefully. Not everyone should access all data. No sharing of IDs or laptops.
     Example: A junior staff should not have access to financial records of the entire company.
5. **Security Governance**
   - Having strong rules, policies, and leadership for security.
   - Good governance ensures that employees follow proper security practices.
     Example: A company regularly updates its security policy, conducts training, and checks systems to reduce cybercrime incidents.

6.1.2 Organizational Implications of Software Piracy

- **Software piracy** is an **Intellectual Property Rights (IPR) violation**.
- The use of pirated software increases serious threats and risks of cybercrime and also computer security.
- This raises legal liabilities, violation of copyright law, and becomes a criminal offence under the Cyber Act.
- The use of unlicensed or pirated software should be discouraged in the organization.
- Cybercriminals use non-genuine computer software, which causes malfunction in computers.
- Non-genuine software can disturb smooth functioning of organizational operations by majorly affecting system security infrastructure.

Reasons why people use pirated software:

1. Pirated software is cheaper and easily available.
2. Many people in organizations or society use pirated software.
3. Latest and updated versions of pirated software are available.

Good Practice:

- The organization should track software licenses to ensure that only genuine copies are used.
- Care should be taken that the number of installations is not more than the allowed number.

6.2 Web Threats for Organizations: The Evils and Perils

- Nowadays, most business applications (shopping, banking, etc.) are **web-based** and many are moving to **cloud computing**.
- E-commerce (online shopping, payments) is growing fast. Audio, video, and software are also delivered from the web.
- Because of this, **cybercriminals use the internet as an easy way to attack companies**.

 Example: Hackers can attack an online shopping website to steal customer credit card details.

6.2.1 Overview of Web Threats to Organizations

- Almost everyone (companies + individuals) is connected to the internet.
- In India, **mobile internet** is very popular → so the risk of web attacks is higher.
- **Workforce mobility** (employees working from different places using internet) creates more challenges for IT managers.
- IT managers must:
    - Protect business data from malware.
    - Ensure enough **bandwidth** (internet speed).
    - Keep websites and applications always **online (uptime)**.

 Example: If an online banking site goes down for even a few hours, customers cannot use it, and the bank loses trust and money.

Types of Web Threats

1. **Employee-related threats**

- Employees may:
  - Visit infected websites.
  - Access unsafe or adult sites.
  - Respond to spam emails.
    Example: An employee clicks on a spam email link that installs malware in the company system.

2. **Management Challenges for IT Managers**
   IT managers face many problems in keeping the web secure and efficient.

Top Challenges

1. **Employee time wasted on internet surfing**
   - Employees waste time browsing social media, watching videos, etc.
   - Organizations need to give **guidelines** (safe computing or internet usage rules).
   - But guidelines alone are not enough—many employees still misuse internet.

   Example: An employee spends 3 hours daily on YouTube during office hours → work productivity goes down.

2. **Enforcing Policy Usage in the Organization**
   - Companies must have **policies** (rules) for internet and data security.
   - A **security policy** is made by senior management to protect data, systems, and employees.
   - A good system allows companies to block harmful or unwanted websites.
   - It keeps a **database of safe/unsafe sites** to protect employees and the company.

Example: Social media sites or gambling sites can be blocked in office computers so employees don't waste time.

3. Monitoring and Controlling Employee Internet Surfing

- Organizations set **rules for internet use**.
- Employees may be allowed to check personal emails only during lunch or break time.
- Special tools (like cookies or monitoring software) are used to track and control how employees use the internet.

Example: A company allows Gmail access only from 1–2 PM but blocks it during office hours to avoid distraction.

---

4. Keeping Security Patches and Virus Signatures Updated

- **Security patches** = fixes provided by software companies to close security holes.

- **Virus signatures** = updated information that helps antivirus detect new viruses.
- If these are not updated regularly, hackers can easily attack.
- Web filters, spam filters, and anti-malware systems must also be updated often for better performance.

 Example: If Windows updates are ignored, hackers can use old weaknesses to enter the system.

---

5. Surviving in the Era of Legal Risk

- If employees visit illegal or offensive websites (like porn sites, pirated software sites), the **company itself may be held responsible** even if management didn't know.
- Company directors can face legal issues for employee misuse.
- If employees visit **illegal or offensive sites** (like porn sites or pirated software), the **directors of the company can be blamed**.
- That's why companies use **web filters and monitoring systems** to reduce such risks.

 Example: If an employee secretly downloads pirated software at work, the company (and its directors) may face legal action.

6. Bandwidth Wastage

- Modern apps, videos, and social media need a lot of **internet bandwidth**.
- When employees use **unwanted apps, downloads, or streaming** during work, it wastes bandwidth and money.
- Companies must **control internet use** during work hours and block non-work websites.

 Example: If 10 employees stream YouTube at the same time, office internet becomes slow → business work suffers.

---

7. Mobile Workers – Security Challenges

- Many employees now work remotely using laptops, mobiles, or PDAs.
- These devices connect to company networks from outside, which makes them harder to monitor.
- Even if the company has strong security inside the office, **remote users can still be weak points**.
- Companies need special tools to protect remote users as well.

 Example: An employee connects office files from home Wi-Fi → if that Wi-Fi is weak, hackers can attack company data.

8. Controlling Access to Web Applications

- Many company apps are now **web-based** or on the **cloud**.
- Sometimes employees **ignore company security rules** → e.g., using **personal email** to send company data.
- Once data leaves the company's system, it's hard to control.
- Organizations must decide **who can access what** (access control).

 Example: An employee uploads secret project files to Gmail → company loses control over that data.

---

9. The Problem of Malware

- Some websites contain **malware (viruses, spyware, ransomware, etc.)**.
- These can infect company systems if visited.
- Companies block known dangerous sites and use **anti-malware tools**.
- But attackers keep changing techniques, so updates are always needed.

 Example: A fake shopping site may install malware when an employee clicks it.

10. Protecting Multiple Offices and Locations

- Today, the **internet connects the whole world**, so companies often have many offices in different countries.
- A single project can be worked on by teams from different locations.
- The big challenge = **keeping data safe and private** in all those places at the same time.
- The solution = use **internet-based security services** (like VPNs, cloud security tools, encrypted communication) to protect every office worldwide.

 Example: An IT company has offices in India, USA, and UK, all working on one project. If security is weak in one office, hackers can attack the whole project.

6.3 Security and Privacy Issues in Cloud Computing

When organizations use **cloud computing**, the main questions are:

- How is data handled on the cloud?
- What kind of **encryption** (data protection) is used?
- Who is responsible if data is lost or leaked?

Storing data in the cloud directly affects **privacy rights** and **data security**.

Three Spheres of Privacy in Cloud Computing

1. User Sphere

- Data is stored on the **user's devices** (computer, laptop, mobile, RFID chips).
- The organization must:
  - Give proper access to users.
  - Monitor usage to stop data misuse.
- Challenges:
  - Data transfer from user → recipient can be unsafe.
  - Weak networks may expose data.
  - Security issues in storing/transferring files.

 Example: An employee uses a laptop with office data. If the laptop is stolen and not encrypted, sensitive information leaks.

---

2. Recipient Sphere

- Data is with the **recipient** (like servers, service providers, or other companies).
- The organization must ensure private data is not **shared or exposed** unnecessarily.
- Challenges:
  - What kind of data is being shared?
  - Can recipients secretly transfer data?
  - Is personal data properly protected?
  - Is data stored temporarily (short-term) or permanently (long-term)?

 Example: A company uses a third-party cloud server. If that server shares customer data with advertisers without permission, privacy is violated.

---

3. Joint Sphere

- Data lies with **web service providers' servers and databases**.
- The main issue = **who owns the data**? The company, the user, or the cloud provider?
- Challenges:
  - Is the user aware of how their data is being used?
  - Can users control or stop misuse of their personal data?

 Example: A user uploads photos to a cloud app. The app provider may use those photos for ads. Does the user still own the photos, or does the company now control them?

6.4 Social Media Marketing: Security Risks and Dangers

- **Social media marketing** = promoting company products or services on platforms like Facebook, Instagram, LinkedIn, Twitter, etc.
- **Social computing** and **social media marketing** are almost the same because both use online tools for communication and promotion.
- Social media is growing very fast and becoming very important for businesses.

Survey of Social Media Use by Businesses (2020)

- **LinkedIn** → used by **76%** of companies.
- **Facebook** → used by **66%** of companies.
- **Twitter** → used by **29%** of companies.
- **Instagram** → used by **17%** of companies.
- **YouTube** → used by **11%** of companies.

 This shows that **LinkedIn and Facebook** are the most popular for business marketing.

Security Risks in Social Media

- Many countries face **data breaches** (stealing of sensitive data).
- Cybercriminals keep a watch on companies' social media activity.
- They try to steal **confidential information** and use it for **financial gain**.
- **Phishing** (fake emails, fake login pages, fake messages) is the **biggest threat**.
- In India, internet use is very high → so **security incidents are also rising**.

How Hackers Attack through Social Media

Hackers use many online channels:

- **Websites**
- **Emails**
- **Instant messaging apps** (like WhatsApp, Messenger)
- **VoIP (Voice over Internet Protocol)** – calling over the internet

Why Organizations Use Social Media Marketing

- It helps companies **promote products and services** directly to users.
- Social media tools (Facebook Ads, Instagram promotions, YouTube ads, etc.) are cheaper and reach more people than traditional marketing.

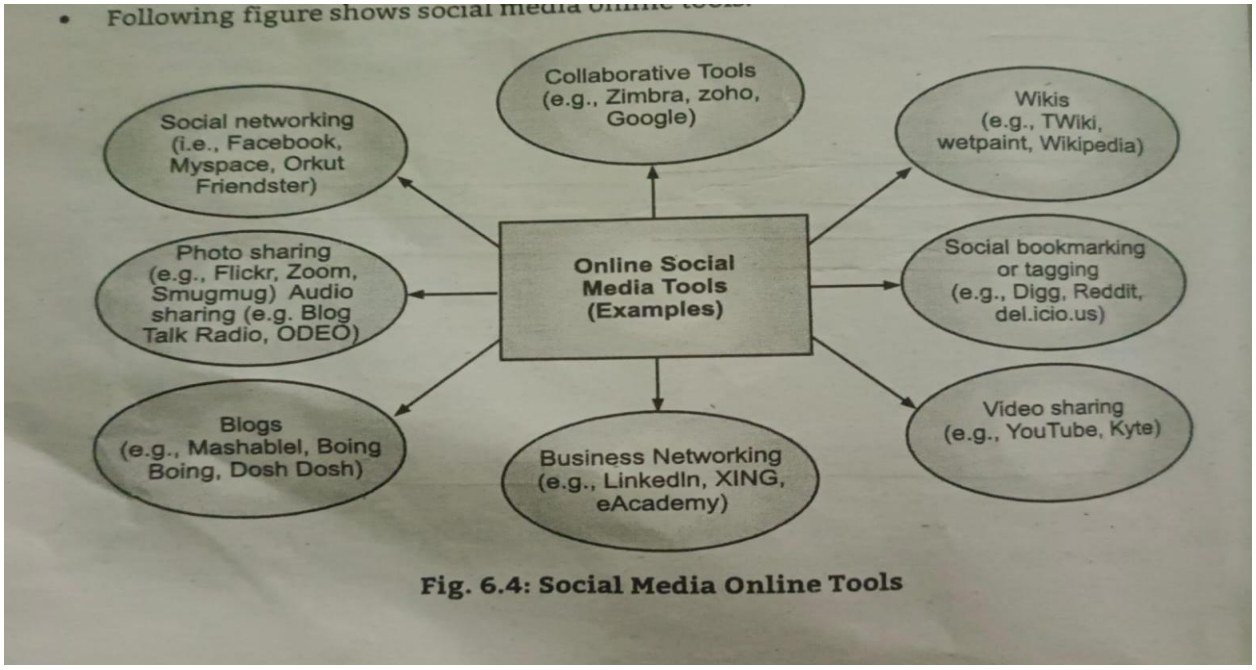

Fig. 6.4: Social Media Online Tools

6.4.1 Understanding Social Media Marketing

Social media marketing became popular because of **internet growth**.
It uses tools like **blogs, Facebook, LinkedIn, Instagram, YouTube, Twitter** to connect with people.

 Why organizations use social media marketing:

1. **Reach more people quickly** – Can promote products/services to thousands or millions at once.
2. **Increase website traffic** – Using blogs and social networking increases the company's **page rank** (visibility on Google).
3. **Save money** – It is cheaper than traditional advertising (TV, newspapers).
4. **Build trust and credibility** – By joining forums, answering customer questions, and giving solutions.
5. **Collect customer data** – Companies can collect **customer profiles** (age, interests, habits) to understand their market better.

6.4.2 Best Practices with Social Media Marketing Tools

Organizations must be careful while using social media. They should follow some **best practices** to stay safe:

1. **Make a Social Media Policy** – Rules for how employees should use social media for work.
2. **Limit blogging for office work** – Personal blogs should not share official information.
3. **Update employees about new threats** – Regular training on phishing, hacking, and scams.
4. **Control data access** – Give access to sensitive data only on a **need-to-know basis**.
5. **Block infected websites** – Use filters to prevent malware from entering.
6. **Use firewalls** – Especially next-generation firewalls for better security.
7. **Fix vulnerabilities** – Do regular **vulnerability scans** to find and patch weaknesses in the system.
8. **Standardize software** – Use only approved, secure versions of software.
9. **Train employees** – Give proper security awareness training.
10. **Have backup plans** – Disaster recovery and contingency planning in case of attacks.
11. **Do risk assessments** – Identify possible threats and prepare for them.
12. **Certification & Accreditation** – Ensure systems meet proper security standards.

6.5 Social Computing and Challenges for Organizations

- **Social computing** = using social media, online tools, and platforms not just for fun, but also for **work, learning, health, business, and communication**.
- It is different from just "social networking for entertainment."
- Businesses use it for **product development, marketing, and sales**.
- But, it also brings **security, safety, and privacy risks**.
- Companies must take **special care** when employees, customers, and suppliers communicate through social platforms.

6.5.1 Protecting People's Privacy in Organizations

- **Privacy and security problems** are often linked to **human mistakes or misuse** (like carelessness, sharing passwords, etc.).
- In the USA → **Social Security Number (SSN)** is used to uniquely identify people.
- In India → **Aadhar Card (UID project)** is used as a unique identity for citizens.
- These IDs must be protected carefully, otherwise **data theft** can happen.

6.6 Organizational Guidelines for Internet Usage & Safe Computing

- Every time employees use the internet, there is a **risk of data leak** → either by accident or by hackers.
- Competitors or cybercriminals can misuse leaked information.
- To avoid this, companies must create **safe computing guidelines** = rules for how employees should use the internet and computers.

6.6.1 Developing an Organizational Policy for Computer Usage

When making such a policy, companies should include:

1. **Mission Statement**
   - A short note about the company's overall goals and purpose.
2. **Introduction**
   - Explains what the policy is about and why it is important.
3. **Internet Safety**
   - Rules about using safe internet practices.
   - Example: using antivirus, firewalls, blocking harmful websites, not downloading unknown files.

4. Confidentiality

- Means **keeping information secret and safe**.
- Only the right people should be able to see or use the information.

5. User Responsibilities

- Every employee must **follow the safe computing rules**.
- Example: not sharing passwords, not downloading pirated software, not visiting unsafe websites.

6. Disciplinary Action

- If someone **breaks the computer usage policy**, the organization can take action against them.
- Example: warning, suspension, or even termination.

7. Miscellaneous Rules

- Other small but important rules should also be mentioned.
- Example: how long a person can use certain facilities, rules for using services like printers, etc.

6.7 Incident Handling: An Essential Part of Cyber Security

- **Incident handling** means what to do when something wrong (like a cyberattack) happens.
- An **incident response system** and a **response team** must be ready to act quickly.

6.7.1 Definitions

- **Incident** → when someone breaks the security rules or something harmful happens to computer systems.
    - Example: hacking, malware attack, or illegal use of company computers.
- **Incident Management** → all the steps to **prevent, control, and fix** such incidents.
- **Cybersecurity** → protecting computers, devices, and data from damage, theft, or misuse.

Three Important Terms

1. **Incident Response** → Immediate action taken when an incident happens. (Like first aid for cyber problems).
2. **Incident Handling** → The full process of managing the incident step by step.
3. **Incident Management** → The bigger system that includes both response and handling, plus prevention.

 All three are connected and work together.

Who Handles Incidents?

- **CSIRT (Computer Security Incident Response Team)** – Special team to handle security issues.
- **IT Group** – The organization's tech team.
- **Security Group** – People responsible for keeping systems safe.

Types of IT Security Incidents

1. **Illegal usage of company's computers or resources**
    - Example: using office internet to mine cryptocurrency.

2. **Unauthorized changes in IT systems or controls**
    - Example: changing security settings without permission.
3. **Spam and mail forgery**
    - Example: sending fake emails pretending to be the com

Why Should an Organization Have an Incident Response Team (IRT)?

1. **Cyberattacks are common**
    - Hackers frequently target organizations to steal personal data (like customer information) and business data (like trade secrets).
    - Example: A hospital's patient records are hacked and leaked.
2. **Quick response is necessary**
    - If an attack is not handled quickly, it can spread and cause bigger losses (money, reputation, customers).
    - Example: A virus attack on one computer may spread to the whole office network if not stopped immediately.
3. **Protect reputation & trust**
    - Customers lose trust if a company cannot protect their information.
    - Example: If a bank fails to stop cyber fraud, customers may move to another bank.
4. **Legal and compliance requirements**
    - Many governments and industries (like banking, healthcare) **require** an incident response system by law.
    - Example: U.S. federal government organizations must follow incident response rules.
5. **Efficient recovery from attacks**
    - An IRT helps the organization recover faster after a cyberattack.
    - Example: Restoring backup data after ransomware instead of paying hackers.
6. **Better preparedness for future**
    - By studying past incidents, the team improves security for the future.
    - Example: After a phishing attack, the IRT may recommend employee training to spot fake emails.

Example of Cyber Security Incidents and information technology infrastructure library prespective.

1. **Unauthorized Access**
    - When someone enters a system without permission.
    - Example: A hacker guesses your email password and logs into your account to read your emails.

---

2. **Inappropriate Usage**
    - When a user uses the system in the wrong way.

- Example: An employee shares illegal software or sends threatening emails using the office computer.

---

3. **Denial of Service (DoS)**
   - An attacker overloads a system so it stops working properly.
   - Example: A hacker sends thousands of fake requests to a company's website, causing it to crash and making it unavailable to real users.

---

4. **Malicious Code (Virus/Worms)**
   - Harmful programs that damage computers or spread quickly.
   - Example: A virus enters through an email attachment and spreads to hundreds of computers in an office, deleting important files.

What Organizations Can Do to Protect Their Systems from Cyber Security Incidents

Organizations need to **protect their important business information** and **personal data** from malware and cyber-attacks. This can be done with proper **IT security planning and management**.

Best Practices for Organizations

1. **Develop and implement malware prevention plans**
   - Create different strategies depending on the type of attack.
   - Example: If ransomware is common, set up data backups and quick recovery systems.

---

2. **Make security policies**
   - Write down clear rules and steps to prevent malware.
   - Example: Company policy may say "Employees should not download unknown apps from the internet."

---

3. **Awareness and training programs**
   - Teach employees and IT staff about how malware spreads and how to avoid it.

- Example: Train staff to recognize phishing emails and not click suspicious links.

---

4. **Documented policies and procedures**
   - Maintain written documents about how to prevent and handle incidents.
   - Example: A checklist on "What to do if malware is detected on a computer."

---

5. **Threat detection capability**
   - Use tools and methods to **detect malware early** before it spreads.
   - Example: Install antivirus software that alerts when it finds a virus.

---

6. **Robust incident response process**
   - Have a system ready to **prepare, detect, and analyze** incidents when they happen.
   - Example: A dedicated IT team that investigates any suspicious activity immediately.

---

7. **Future-proof protection**
   - The organization should prepare for both current and future threats.
   - Example: Updating firewalls and antivirus regularly to stop new malware types.

? Incident Response Team (IRT) – Work, Capability & Structure

- An **Incident Response Team** is a group responsible for handling cyber incidents.
- They need to have **skills, training, and proper tools**.
- Their job is to:
  1. Detect and analyze incidents.
  2. Respond quickly to reduce damage.
  3. Coordinate efforts between different departments.
  4. Prepare for future incidents.

 Example:
If a company's website is hacked, the Incident Response Team will:

- Detect the hack,
- Stop the attack,
- Recover the system,

- Investigate how it happened,
- Prevent it from happening again.

6.7.7 Benefits from Incident Response System

An **Incident Response System (IRS)** is a structured way to deal with cyber incidents (like hacking, malware, data theft).

1. **Systematic Response**
   - The organization can handle incidents in an organized way.
   - Example: Instead of panicking during a virus attack, the company follows a fixed plan step by step.
2. **Faster Recovery**
   - Helps employees recover quickly from an incident and reduces data loss.
   - Example: If files are encrypted by ransomware, backups are restored quickly to avoid long downtime.
3. **Useful Information for Future**
   - The data collected during incident handling can be used later to prevent similar problems.
   - Example: If hackers used a weak password, the company learns and enforces stronger passwords in the future.
4. **Better User Satisfaction**
   - If problems are handled properly, customers and employees trust the system more.
   - Example: Users feel safe if their bank immediately blocks fraud attempts on their accounts.
5. **Efficient Use of Staff**
   - IT staff can work more effectively with proper procedures.
   - Example: Service desk staff know exactly what to do when they get a malware complaint.
6. **Measure and Monitor IT Performance**
   - Helps track how well the IT system is performing.
   - Example: Monitoring service downtime during incidents improves service agreements (SLA).
7. **Better Decisions by Management**
   - Provides good data for decision-making about security.
   - Example: Reports show increasing phishing attacks → management decides to invest in better email filters.
8. **Track Incidents Easily**
   - Makes it easier to record and analyze incidents.
   - Example: A logbook of all past cyber incidents helps track patterns.

6.7.8 Checklists

A **checklist** = list of steps/things you must follow during an incident.
It ensures nothing important is missed.

Examples of checklists:

- Checklist for first response (what to do first when incident happens).
- Generic checklist for all incidents.
- Checklist for handling **DoS attacks**.
- Checklist for handling **malicious code or unauthorized access**.
- Security review checklist.
- Computer incident reporting form.

 Example: If a virus is found, a checklist may include:

1. Disconnect computer from network,
2. Run antivirus scan,
3. Report to IT team,
4. Document the incident.

6.8 Intellectual Property (IP) in Cyberspace

- **Intellectual Property (IP):** Anything **created by the human mind** that has value and can be owned legally.
- IPR = **Legal rights** given to protect those creations.
- It is a type of **intangible property** (you can't touch it like land or money, but it has value).

Examples of IP:

- **Copyright** → books, music, movies, art.
- **Patent** → inventions, new technology.
- **Trademark** → logos, brand names.
- **Trade secrets** → secret formulas (like Coca-Cola recipe).

 In cyberspace, protecting IP is very important because:

- Digital files (songs, movies, software) can be copied or stolen easily.
- Hackers may steal inventions or business secrets.

Example:

- A software company's program gets pirated and shared online → violation of **copyright**.

- A hacker steals secret designs of a new smartphone → violation of **trade secret**.

Types of Intellectual Property (IP)

1. **Copyrights**
2. **Patents**
3. **Trademarks**
4. **Trade Secrets**
5. **Trade Name**
6. **Domain Name**

Copyrights

- **Meaning:** Copyright is a **legal protection** given to the creator of original work (like books, songs, movies, drawings, or computer programs).
- It protects the **expression of an idea**, not the idea itself.

 Example:

- If you write a poem, you own the copyright.
- Someone else cannot copy and publish it as their own.
- But the *idea* of writing about "love" or "rain" is not protected – only your unique poem is.

---

2. **Automatic Protection:**
    - The moment you create something and fix it in some form (write it down, record it, paint it), it is automatically protected.
    - No need to publish it first.

    Example: If you write a story in your notebook, it is automatically under copyright.

---

3. **Rights of the Copyright Owner:**
    - Copy the work (make books, CDs, etc.).
    - Create new works based on it (like a movie sequel).
    - Distribute copies.
    - Perform or display it publicly.

    Example: A singer can stop others from selling copies of their songs without permission.

4. **Infringement (Violation):**
    - If someone uses copyrighted work without permission, it is copyright infringement.

    Example: Downloading pirated movies or songs is copyright infringement.

---

5. **Fair Use (Exceptions):**
    - Some uses are allowed without permission:
        - For education/non-commercial use.
        - For criticism, commentary, or parody.

    Example: A teacher showing a small clip of a movie in class for learning purposes = fair use.

---

6. **Duration of Copyright:**
    - Protection lasts for the **author's lifetime + 70 years after death**.

    Example: If an author dies in 2025, their book remains copyrighted until 2095.

Patents

- A **patent** is a legal right given to an **inventor** to protect their invention.
- It gives the inventor the **exclusive right** to stop others from **making, using, selling, or importing** the invention without permission.

 Example: If you invent a new type of electric car engine, only you (or your company) can make and sell it. Others need your permission (license).

Duration of a Patent

- **Utility patent** → lasts **20 years** from the date of filing.
- **Design patent** → lasts **14 years** from the date it is granted.
- After expiry, the invention goes into the **public domain** (anyone can use it freely).

 Example: The original telephone patent by Alexander Graham Bell expired long ago, so now anyone can make telephones.

□ Rights of a Patent Owner

- You can **exclude others** from copying or using your invention.
- You can **license** the invention to others (and earn money).
- You can **sue** someone if they use your invention without permission.

□□ Note: The inventor must **enforce** the patent themselves (the Patent Office doesn't do it for them).

□ Types of Patents

1. **Utility Patents**
   - For new and useful processes, machines, chemical compositions, or improvements.
   - Example: A new medicine, a water-purifying machine, or a faster engine.
2. **Design Patents**
   - For new, original, and decorative designs of products.
   - Example: The unique design of an iPhone, or the shape of a Coca-Cola bottle.
3. **Plant Patents**
   - For inventing or discovering and reproducing a new variety of plant.
   - Example: A new hybrid mango tree developed by scientists.

Special Case: Software & Business Method Patents

- **Software Patents:**
  - Very controversial because not all countries agree if software is an "invention."
  - Issues: Does patenting software **help innovation** or **block progress**?
  - Example: A unique algorithm for data compression may be patented.
- **Business Method Patents:**
  - Protect new ways of doing business (e-commerce, banking, insurance).
  - Example: Amazon's "1-Click Ordering System" was once patented.

Simple Real-life Examples:

- **Utility Patent:** A new COVID-19 vaccine formula.
- **Design Patent:** The look and shape of the Nike Air Jordan shoe.
- **Plant Patent:** A new type of rose that never existed before.

- **Software Patent:** Google's PageRank algorithm for search results.
- **Business Method Patent:** PayPal's online payment system.

---

3. Trademarks (Service Marks)

- A **trademark** is a **symbol, word, logo, or design** that identifies a company's **product** and makes it different from others.
- A **service mark** is the same thing, but it is used to identify a **service** instead of a product.

 Example:

- **Trademark (product):** Nike's ✔ **(swoosh logo)** → identifies Nike shoes.
- **Service Mark (service):** McDonald's golden **"M" logo** → identifies its food services.

Key Points about Trademarks:

1. **Who can own it?**
   - An individual, business, or any legal entity.
2. **Where is it used?**
   - On product packages, labels, advertisements, or the product itself.
3. **Validity:**
   - A registered trademark is valid for **10 years**.
   - It can be **renewed every 10 years** as long as it is being used.
4. **Maintenance:**
   - The owner must file an affidavit (legal statement) between the **5th and 6th year** after registration, and then every 10 years, to prove it is still being used.
   - If not used, others can take it.
5. **Value:**
   - A strong trademark builds **brand identity** and **customer trust**, helping a company keep its market share.

Real-life Examples:

- Apple's **logo** = trademark for its electronics.
- Coca-Cola's **name and logo** = trademark for soft drinks.
- KFC's **"It's Finger Lickin' Good"** slogan = trademark.
- Airtel's **"wave" logo** = service mark for telecom services.

🔒 4. Trade Secrets

- A **trade secret** is **valuable business information** that companies keep secret to stay ahead of competitors.
- Unlike patents, **trade secrets are not registered** – they must be kept confidential.
- If someone leaks or steals a trade secret, it is illegal.

🔍 What can be a Trade Secret?

- Recipes
- Marketing plans
- Financial data
- Customer lists
- Manufacturing processes

🔹 Examples:

- **Coca-Cola Recipe** → kept secret for more than 100 years.
- **Google Search Algorithm** → closely guarded trade secret.
- **KFC's Secret Spice Mix** → trade secret that makes their chicken unique.

⚖️ Difference between Patent & Trade Secret:

- **Patent:** Publicly registered, lasts for 20 years, after expiry anyone can use it.
- **Trade Secret:** Never expires (as long as it stays secret), but if revealed, anyone can use it.

🔹 Example:

- A **new medicine formula** → better protected as a patent.
- A **soft drink recipe** → better protected as a trade secret.

---

5. Trade Name (Business Name)

- A **trade name** (or business name) is simply the **official name of a company** under which it does business.
- It identifies the **business itself**, not the products or services.
- It is registered for legal and commercial purposes (like contracts, licenses, taxation).

- **No automatic exclusive rights** are given to a trade name unless it is also registered and used as a **trademark**.

 Example:

- **"Parle Products Pvt. Ltd."** → This is a **trade name** (the company name).
- **"Parle-G" biscuits** → This is a **trademark** (the brand name for products).
- **Infosys Limited** → Trade Name.
- **Infosys logo** → Trademark.

 Key Point:

- Trade Name = Company's official name.
- Trademark = Brand identity (products/services).

---

6. Domain Name

- A **domain name** is the **online identity** of a business.
- Every computer on the Internet is identified by an **IP address** (like `74.125.127.147`), but since numbers are hard to remember, we use **domain names** instead.
- The **Domain Name System (DNS)** converts names into IP addresses so that websites can be found easily.

 Example:

- IP Address: `74.125.127.147`
- Domain Name: `www.google.com` → easier to remember.

 Importance of Domain Names:

1. Helps customers find your business online.
2. Protects brand identity (e.g., `www.nike.com` matches the Nike brand).
3. A domain name can become as valuable as a **trademark** because it represents the business on the internet.

Domain Names & Ownership

- A **domain name** (like `www.amazon.com`) helps people find a business online.
- **But** registering a domain name does **not automatically give ownership rights** like a trademark.
- That's why issues like **cybersquatting** happen.

Cybersquatting

- **Meaning:** Cybersquatting is when someone **registers a domain name** (website address) that is **identical or very similar** to an existing **trademark, brand, or personal name**—with the **bad intention** of selling it later for profit.

 Example:

- Nike's real website = `www.nike.com`
- A cybersquatter registers `www.nike-shoes.com` or `www.niike.com` and tries to sell it back to Nike at a high price.

This is illegal because they are trying to **profit from someone else's brand name or reputation**.

Anti-Cybersquatting Laws

- To protect businesses and consumers, laws have been made.
- The most important one is the **Anti-Cybersquatting Consumer Protection Act (ACPA)** in the USA.
- The ACPA prohibits registering domain names that are:
  - Identical or confusingly similar to a trademark or personal name.
  - Done with **bad faith intent** (to profit unfairly).

 Example:

- If someone registers `www.facebook-login.com` to trick people and later sell it to Facebook → ACPA protects Facebook.

Key Takeaways

1. **Domain names ≠ ownership rights** (only registration, not permanent property like trademark).
2. **Cybersquatting = illegal** registration of domains to misuse someone's brand or name.
3. **ACPA law** protects businesses and trademark owners against cybersquatting abuses.

 Real-life Example:

- In 1999, a cybersquatter registered **`peta.org`** (People for the Ethical Treatment of Animals).
- Instead of animal rights, the site showed **"People Eating Tasty Animals"** □.
- PETA sued under ACPA and won the rights to the domain.
