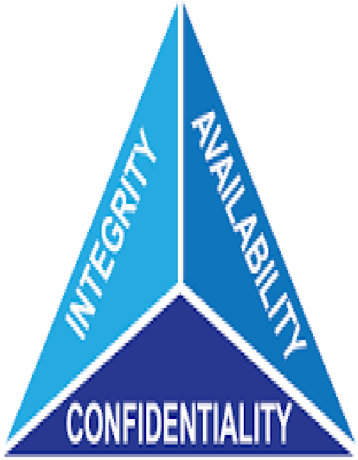


IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

PMCA605L : Cyber Security

Module 6: CyberSecurity - Organizational Implications

Courtesy: Nina Godbole, Sunit Belapure & *Other Sources of Internet*

VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Dr. R. K. Nadesh

Introduction

- Global Environment with continuous network connectivity.

- The possibilities for cyberattacks can emanate from sources that are local, remote, domestic, or foreign.

- They could be launched by an individual or a group.

- They could be casual probes from hackers using personal computers (PCs) in their homes, hand-held devices, or intense scans from criminal groups

Cyber Security Perspective

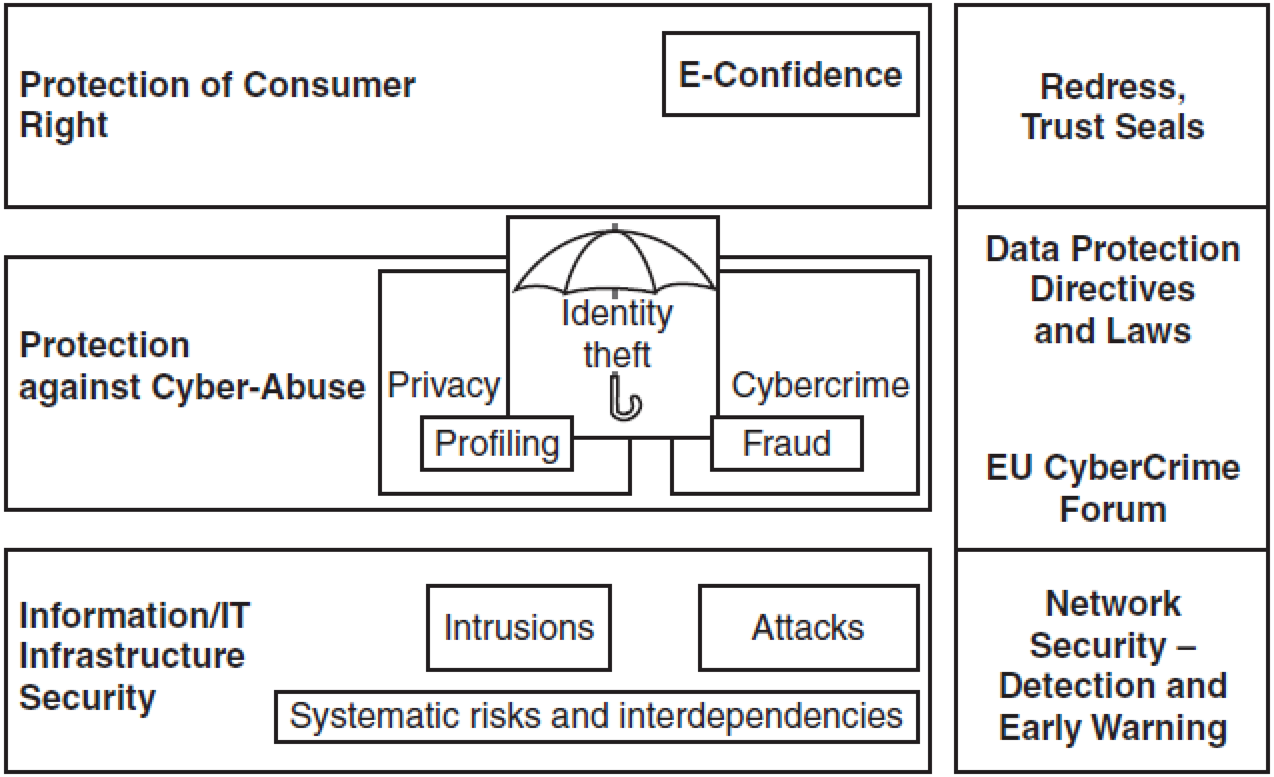

Protection of Consumer Right
E-Confidence
Redress, Trust Seals
Protection against Cyber-Abuse
Privacy
Identity theft
Cybercrime
Profiling
Fraud
Data Protection Directives and Laws
EU CyberCrime Forum
Information/IT Infrastructure Security
Intrusions
Attacks
Systematic risks and interdependencies
Network Security – Detection and Early Warning

Figure 1 | A cybersecurity perspective. EU is the European Union.

PI can be any of the following data

1. Social security number (SSN)/social insurance number.

2. Driver's license number or identification card number.

3. Bank account number, credit or debit card number with personal identification number such as an access code, security code or password that would permit access to an individual's financial account.

4. Home address or E-Mail address.

5. Medical or health information.

Insider Threats

- Malicious Insider – Comprises CIA Triad
- Careless Insider – Negligence (Mistake)
- Tricked Insider - Social Engineering

Four Key Dimensions of Privacy

1. Informational/data privacy
2. Personal privacy
3. Communication privacy
4. Territorial privacy

Informational/data privacy

- **Refers to the protection of personal data from unauthorized collection, processing, and distribution.**

- **It is about data protection, and the user's rights to determine how, what, and to what extent information about them is communicated to other parties.**

Examples:

•Online banking and financial data protection.

Threats & Challenges: **Facebook-Cambridge Analytica Scandal (2018)**

✓ Data breaches and hacking.
✓ Unauthorized data collection by companies.
✓ Misuse of AI for personal profiling.

Personal Privacy

- Protection of an individual's **personal choices, and biometric data** from unauthorized interference.

Examples: Aadhaar Data Breach (India, 2018)

- Fingerprint and facial recognition in smartphones (e.g., Face ID, Aadhaar authentication).
- **Medical privacy**: Patients' health data should remain confidential.
- **Surveillance concerns**: Excessive CCTV monitoring invades personal space.

Threats & Challenges:

✓ Biometric data leaks (e.g., Aadhaar data exposure).
✓ Excessive surveillance by governments or corporations.
✓ Medical data sharing without consent.

Communication Privacy

- **Ensures that personal communications (emails, calls, chats, messages) remain confidential and are not intercepted without consent.**

Examples: WhatsApp Pegasus Spyware Attack (2019)

•End-to-end encryption in WhatsApp.

•Wiretapping concerns in government surveillance

•Corporate email monitoring without employee consent.

Threats & Challenges:

✓ Phishing attacks exposing private emails.

✓ Data leaks from messaging apps.

Territorial Privacy

Refers to physical privacy, ensuring individuals have control over their personal spaces (home, workplace, digital spaces) without intrusion.

Examples: **Google Street View Privacy Violations**

- Drones & hidden cameras invading private properties.
- Smart home devices (Alexa, Google Home) listening without consent.
- Employers tracking employees through GPS-based monitoring.

Threats & Challenges:

✓ Unauthorized home surveillance.
✓ GPS tracking without consent.
✓ Workplace monitoring without transparency.

Key challenges from emerging new information threats to organizations:

1. Industrial espionage
2. IP-based blocking
3. IP-based “cloaking”
4. Cyberterrorism
5. Confidential information leakage

Industrial Espionage

- The act of spying on competitors or organizations to gain confidential business information, trade secrets, or proprietary data.

- This can involve hacking, insider threats, or physical theft of sensitive materials.

IP-Based Blocking

- A security measure that restricts access to a website or network based on the visitor's IP address.
- It's often used to prevent cyberattacks, enforce geo-restrictions, or block malicious users.
- However, attackers can bypass it using VPNs or proxy servers.

IP-Based “Cloaking”

- A technique where websites or services show different content based on the visitor's IP address.

- Hackers might use this to deceive cybersecurity measures by showing legitimate content to security analysts while delivering harmful content to real users.

Cyberterrorism

- The use of digital attacks to disrupt, damage, or threaten critical infrastructure, businesses, or governments for political, ideological, or economic reasons.

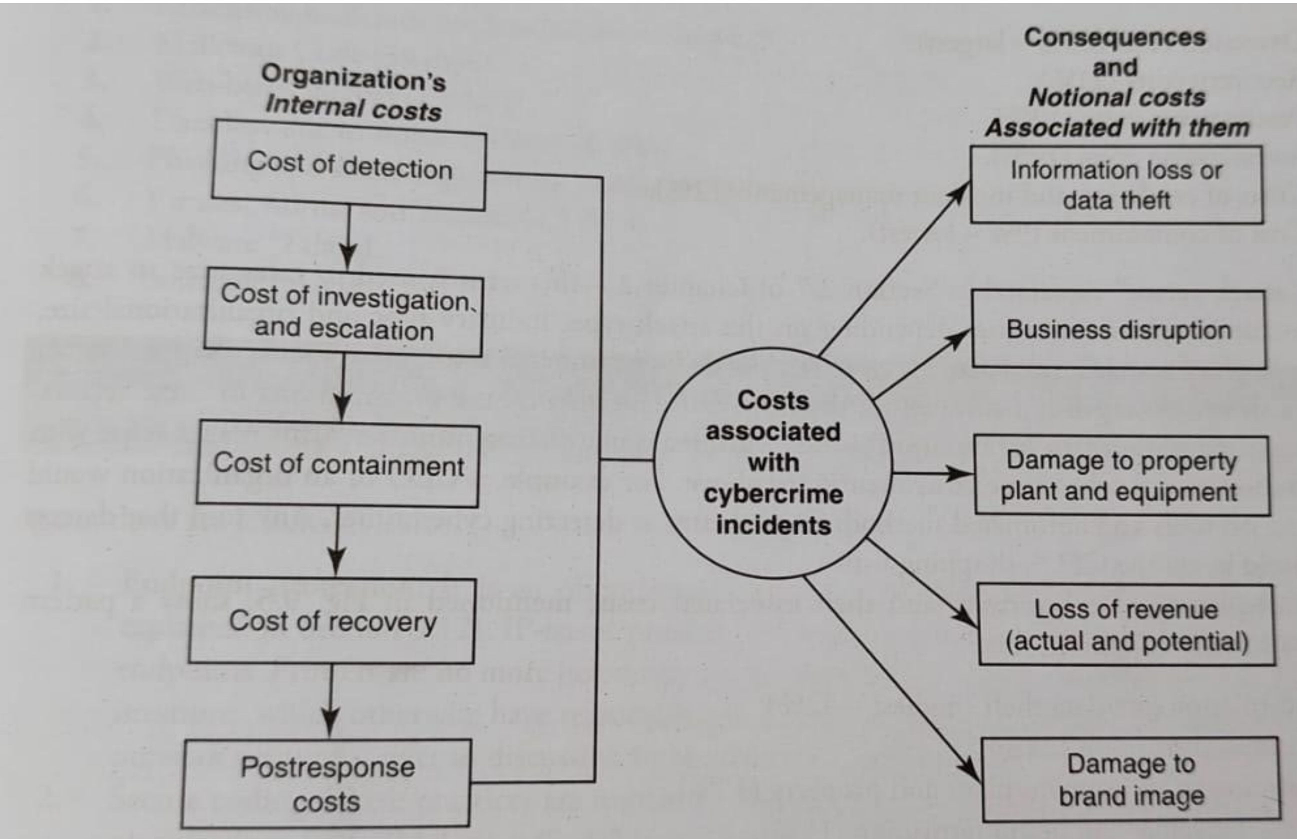
- Examples include hacking power grids, launching DDoS attacks on government websites, or spreading propaganda.

Confidential Information Leakage

- The unintentional or intentional exposure of sensitive business or personal data.

- This can happen through insider threats, phishing attacks, data breaches, or even poorly secured cloud storage.

Cost of Cybercrimes and Intellectual Property Rights (IPR)



Organization's *Internal costs*

Cost of detection

Cost of investigation and escalation

Cost of containment

Cost of recovery

Postresponse costs

Costs associated with cybercrime incidents

Consequences and *Notional costs Associated with them*

Information loss or data theft

Business disruption

Damage to property plant and equipment

Loss of revenue (actual and potential)

Damage to brand image

Figure 9.5 | Cost of cybercrimes.

Consequences of cybercrimes and their associated costs

1. Information loss/data theft (highest – 42%).

2. Business disruption (22%).

3. Damages to equipment, plant, and property (13%).

4. Loss of revenue and brand tarnishing (13%).

5. Other costs (10%).

Organizational Implications of Software Piracy

✓ Software piracy is an IPR violation crime.

✓ Use of pirated software increases serious threats and risks of cybercrime and computer security. Violation of copyright laws (pirated software).

✓ *Knowing use* is also a criminal offense under the Act.

✓ Use of unlicensed software (pirated software) should be discouraged.

✓ Vulnerability of nongenuine computer software. The spread of this virus can be partly attributed to the lack of automatic security updates for unlicensed software.

Organizational Implications of Software Piracy

- Organizations should track software licenses to ensure that only genuine copies are used and that the number of installations is not more than the allowed number by establishing a software license tracker tool.

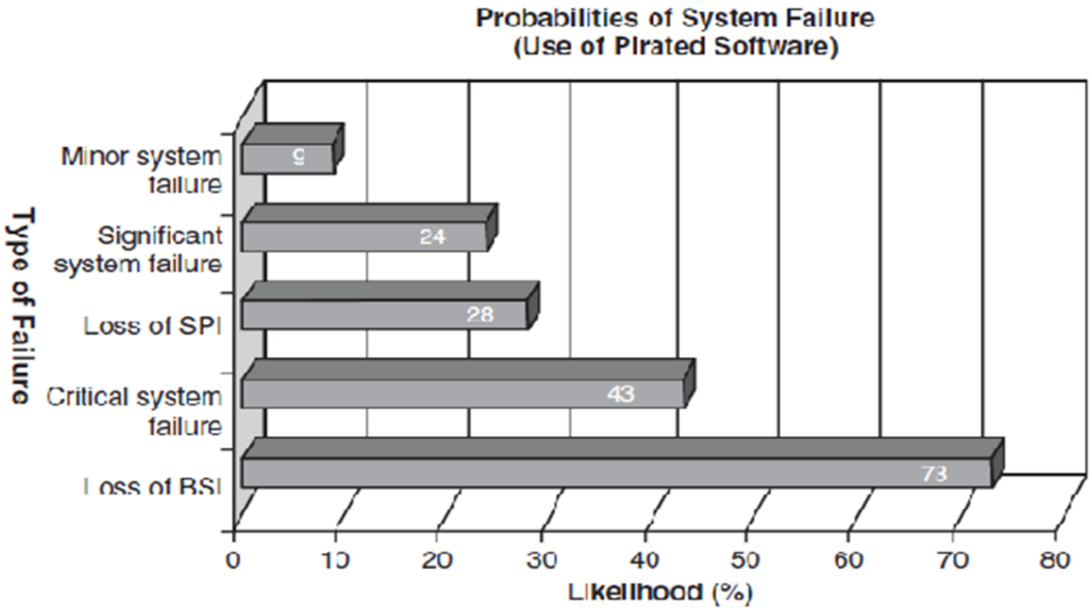


Figure 3 Probabilities of system failure (use of pirated software). SPI is sensitive personal data and BSI is business sensitive information.

Web Threats to Organizations

- Large number of companies as well as individuals have a connection to the Internet.
- Employees expect to have Internet access at work just like they do at home.
- Mobile workforce has various categories.
- Workforce mobility poses challenges for IT managers whose agenda is to protect the business and business assets against malware.
- Protection of information assets is important; especially protection of removable/detachable media.

Categories of Web threats

1. Employees do a number of activities online (viz., visiting infected websites, responding to Spam mails and attempting to hack sites) to name a few.

2. There are many challenges and difficulties IT managers face when it comes to managing web use in a secure and efficient way and when it comes to handling an “incident” alert received.

Web Threats

- Web threats refer to **cyber risks originating from the internet**, including **phishing, malware, ransomware, data breaches, DoS attacks, and identity theft**.

- Organizations and individuals are vulnerable to these attacks due to **poor cybersecurity measures, social engineering tactics, and software vulnerabilities**.

Types of Web Threats:

✓ **Phishing** – Fake websites/emails trick users into revealing credentials.

✓ **Malware & Ransomware** – Malicious programs encrypt or steal data.

✓ **Man-in-the-Middle (MitM) Attacks** – Intercepting data between users and servers.

✓ **SQL Injection (SQLi)** – Hackers inject malicious SQL queries to access databases.

✓ **Denial of Service (DoS/DDoS**) – Overloading servers to make services unavailable.

✓ **Zero-Day Exploits** – Attacks on unknown software vulnerabilities.

Employee Time Wasted on Internet Surfing

1.Approximately 45–60 minutes spent on personal web surfing at work.

2.Safe Computing Guidelines/Internet Usage Guidelines should be implemented.

3. Organizations need software tools to track.

Bandwidth Wastage Issues

- Organizations have to pay for their bandwidth utilization.

- Under such a scenario, there is a concern when expensive bandwidth is wasted by non-work Internet use.

- With the rise of social networking and the trend toward social media marketing, streaming audio and video sites, and TV-on-demand business, Internet connections are under severe strain.

- There are tools to protect an organization’s bandwidth by stopping unwanted traffic before it even reaches your Internet connection.

Keeping Security Patches and Virus Signatures Up to Date

- ✓ Updating security patches and virus signatures has now become a reality of life and a necessary activity for safety in the cyber world!
- ✓ Keeping security systems up to date with security signatures, software patches, etc. is almost a nightmare for management.
- ✓ Not doing it properly exposes IT systems to unnecessary risk.
- ✓ In-house web filters, policy engines, Spam, and anti-malware systems need regular updates to stay effective.
- ✓ Finding IT technicians with the right level of skill to manage these systems is another aspect of this problem.

Need for Protecting Multiple Offices and Locations

- Delivery from multi-locations and teams collaborating from multi-locations to deliver a single project is a common working scenario today.
- Most large organizations have several offices at multiple locations.
- Protecting information security and data privacy at multiple sites is indeed a major issue primarily because protecting a single site itself is a challenge these days.
- In a solo site scenario, anti-malware, web filtering, and monitoring software are needed.
- Additional effort is required with multiple sites, as all hardware and administrative overheads are multiplied!
- For an Internet-based-hosted service, it does not matter how many E-Mail servers there are. However, with in-house solutions, you do not have to pay an upfront capital cost for hardware and software followed by an unpredictable ongoing maintenance cost. A fixed fee per user is also an option to consider.

Security and Privacy Implications from Cloud Computing

Social Computing and Its Challenges

- **Social computing** refers to the use of digital platforms that enable **human interaction, collaboration, and communication** through technology.

- It includes **social media, online communities, blogs, wikis, collaborative tools, and crowdsourcing platforms**.

Examples:

Facebook, Twitter, Instagram (Social Media)
Wikipedia (Collaborative Knowledge Sharing)
GitHub (Social Coding & Open Source Development)
Amazon (User Reviews & Ratings)

Key Challenges in Social Computing

1. Privacy & Data Security Risks

Issue: Users share large amounts of personal data on social platforms, making them vulnerable to **data breaches, identity theft, and surveillance**.

2. Spread of Misinformation & Fake News

Issue: Social media allows **false information and fake news** to spread rapidly, affecting public opinion, elections, and even health (e.g., COVID-19 misinformation).

3. Cyberbullying & Online Harassment

Issue: Social platforms allow anonymity, leading to **cyberbullying, trolling, and online harassment**

Key Challenges in Social Computing

4. Addiction & Mental Health Issues

Issue: Social media platforms are designed to be addictive, leading to **anxiety, depression, and decreased productivity**.

The "fear of missing out" (**FOMO**) and excessive screen time impact mental health.

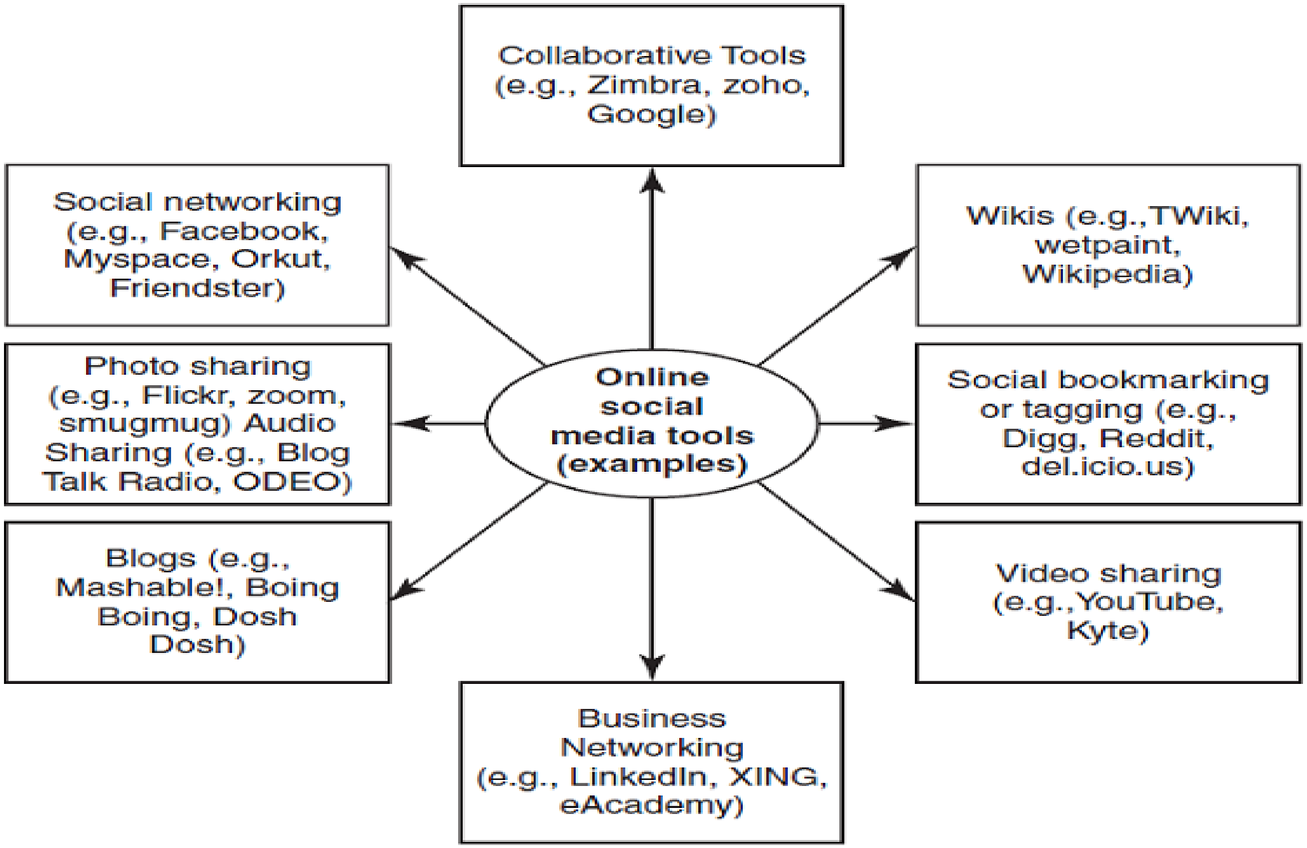
5. Lack of Digital Literacy & Awareness

Issue:. Many users do not understand **how social computing platforms operate, leading to data privacy risks, misinformation spread, and online scams**.

Example:

- **Phishing attacks through fake Facebook ads** steal user credentials.
- **Elderly users fall victim to WhatsApp fraud scams**.

Social Media Tools



Online social media tools (examples)

Collaborative Tools (e.g., Zimbra, zoho, Google)

Social networking (e.g., Facebook, Myspace, Orkut, Friendster)

Wikis (e.g.,TWiki, wetpaint, Wikipedia)

Photo sharing (e.g., Flickr, zoom, smugmug) Audio Sharing (e.g., Blog Talk Radio, ODEO)

Social bookmarking or tagging (e.g., Digg, Reddit, del.icio.us)

Blogs (e.g., Mashable!, Boing Boing, Dosh Dosh)

Video sharing (e.g.,YouTube, Kyte)

Business Networking (e.g., LinkedIn, XING, eAcademy)

Figure 4 | Social media – online tools.

Social Media Marketing

1. Facebook is used by 37% of the organizations.
2. LinkedIn is used by 36% of the organizations.
3. Twitter is used by 36% of the organizations.
4. YouTube is used by 22% of the organizations.
5. MySpace is used by 6% of the organizations.

Understanding Social Media Marketing

1. To be able to reach to a larger target audience.

2. To increase traffic to their website coming from other social media websites.

3. To reap other potential revenue benefits and to minimize advertising costs.

4. To build credibility by participating in relevant product promotion forums and responding to potential customers' questions immediately.

5. To collect potential customer profiles.

Privacy Implications in Social Media Marketing

Data Collection & User Privacy

- A social media platform collects extensive user data, including location, browsing history, and personal preferences, to provide targeted advertisements.

Privacy Risks of Third-Party Application

- A mobile game that integrates with Facebook asks for access to contacts, messages, and location. Later, users discover that their data was shared with advertisers without their consent.

Privacy Implications in Social Media Marketing

➢ Ethical Issues in Targeted Advertising

- An e-commerce company uses AI-powered algorithms to analyze user data and deliver highly personalized advertisements. However, some users feel this is an invasion of privacy as ads appear based on private conversations.

➢ Social Media Influencers & Deceptive Marketing

- A popular influencer promotes a health supplement without disclosing that they were paid for the endorsement. Later, it is discovered that the product has harmful side effects.

Privacy Implications in Social Media Marketing

Data Leaks & Consumer Trust in Social Media Marketing

- A well-known fashion brand runs a marketing campaign through social media ads, but a data breach exposes customer emails and phone numbers. Customers start losing trust in the brand.

Fake Reviews & Social Media Brand Manipulation

- A travel company pays **fake reviewers** to leave **positive reviews on social media** about their services. Customers later realized the reviews were misleading.

Best Practices with the Use of Social Media Marketing Tools

- Establish a “social media policy.”
- Use of personal blogging for work-related matters should be monitored and minimized.
- Use of policies and implementation of policy-based procedures are always essential.
- Increasing employee awareness is an ongoing activity.
- Organizations need to educate their employees about the risks associated with the use of online social media tool.
- Organizations must raise their employees’ awareness of the fact that even seemingly innocuous information can reveal too much about the company or the person’s private life.
- It is worth exploring the appointment of a social media expert within the company.
- Blocking the infected websites is another necessary activity.
- Access blocking can also be applied to any other suspicious site on the Internet.

Social Computing and the Associated Challenges for Organizations

- Social computing (or “Web 2.0”): Empowers people to use Web-based public products and services.

- It is much more than just individual networking and entertainment.

- It helps thousands of people across the globe to support their work, health, learning, getting entertained, and citizenship tasks in a number of innovative ways.

- Social networking, social media marketing, and social computing are not unrelated concepts.

- Social computing is related to social media marketing.

- Due care is to be taken while using social computing as a channel strategy for communicating with internal or external stakeholders.

Protecting People's Privacy

- ✓ People hate to be monitored
- ✓ Tracking and monitoring people's transactions on the Internet is a controversial issue.
- ✓ RFIDs have been successful in tracking objects, animals, birds, and goods in shipment.
- ✓ The Social Security Number is a well-established system/mechanism for uniquely identifying all citizens
- ✓ When the unique identity database comes into existence, the number of identity databases (voter ID, passports, ration cards, licenses, fishing permits, border area ID cards) currently are supposed to be linked to it.

Developing an Organizational Policy for Computer Usage

A “computer usage policy” should address the following elements:

1. Mission Statement
2. Introduction
3. Internet Safety
4. Confidentiality
5. User Responsibilities
6. Disciplinary Action for Privacy Violation and Disclaimer
7. Miscellaneous

Incident

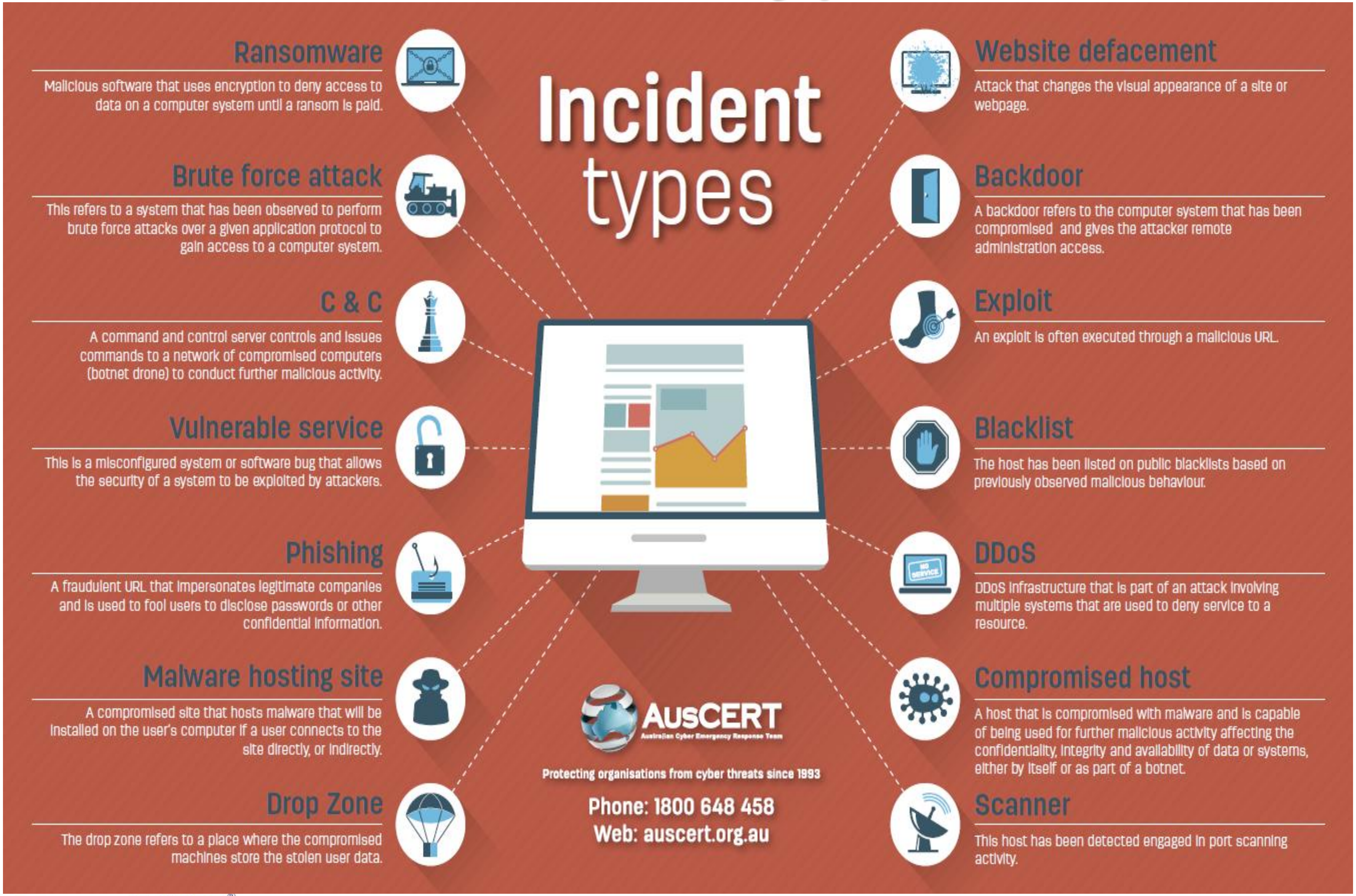
1. Loss of computing devices

2. Detection or discovery of a program agent

3. Detection or discovery of unauthorized users, or users with privileges in excess of authorized privileges

4. Detection or discovery of critical or widespread vulnerabilities, or misconfiguration

Incident Types



Incident types

Ransomware

Malicious software that uses encryption to deny access to data on a computer system until a ransom is paid.

Brute force attack

This refers to a system that has been observed to perform brute force attacks over a given application protocol to gain access to a computer system.

C & C

A command and control server controls and issues commands to a network of compromised computers (botnet drone) to conduct further malicious activity.

Vulnerable service

This is a misconfigured system or software bug that allows the security of a system to be exploited by attackers.

Phishing

A fraudulent URL that impersonates legitimate companies and is used to fool users to disclose passwords or other confidential information.

Malware hosting site

A compromised site that hosts malware that will be installed on the user's computer if a user connects to the site directly, or indirectly.

Drop Zone

The drop zone refers to a place where the compromised machines store the stolen user data.

Website defacement

Attack that changes the visual appearance of a site or webpage.

Backdoor

A backdoor refers to the computer system that has been compromised and gives the attacker remote administration access.

Exploit

An exploit is often executed through a malicious URL.

Blacklist

The host has been listed on public blacklists based on previously observed malicious behaviour.

DDoS

DDoS infrastructure that is part of an attack involving multiple systems that are used to deny service to a resource.

Compromised host

A host that is compromised with malware and is capable of being used for further malicious activity affecting the confidentiality, integrity and availability of data or systems, either by itself or as part of a botnet.

Scanner

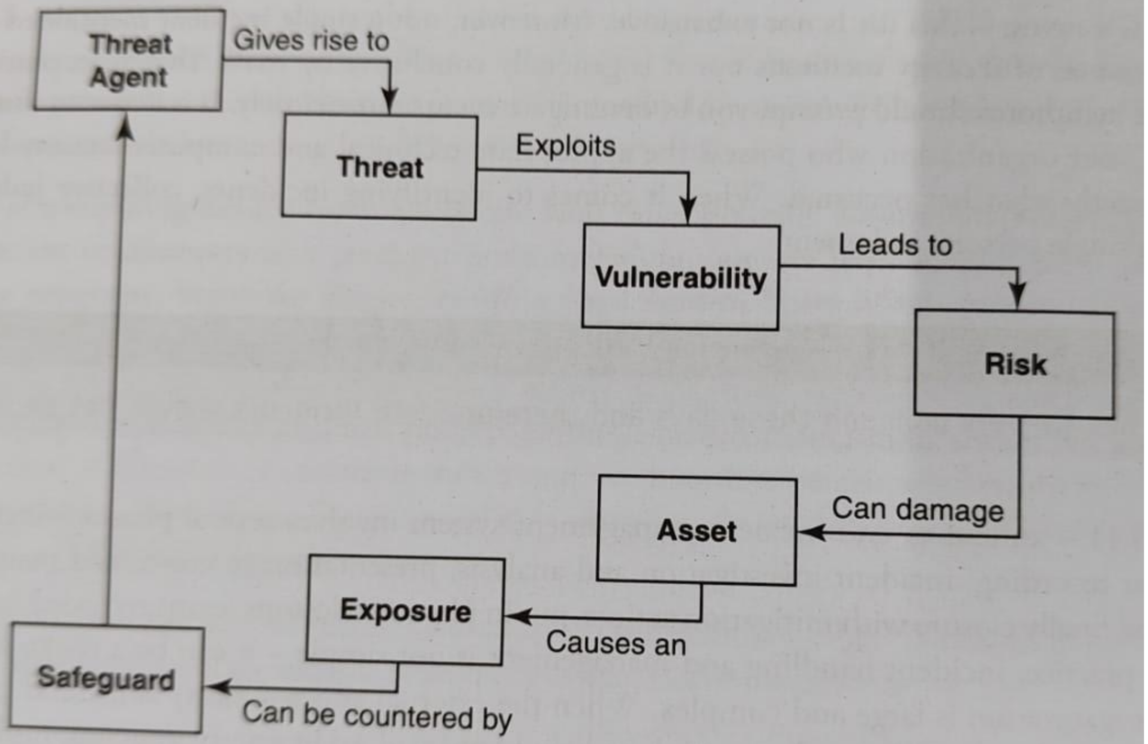
This host has been detected engaged in port scanning activity.

AusCERT
Australian Cyber Emergency Response Team

Protecting organisations from cyber threats since 1993

Phone: 1800 648 458
Web: auscert.org.au

Threats, Vulnerabilities, Assets and Risks



Threat Agent
Gives rise to
Threat
Exploits
Vulnerability
Leads to
Risk
Can damage
Asset
Causes an
Exposure
Can be countered by
Safeguard

Figure 9.13 | Threats, vulnerabilities, assets and risks.

Incident Handling

- Handling of any type of service disruption or interruption.
- The act of violating an explicit or implied security policy.
- An adverse event in an information system, and/or network, or the threat of the occurrence of such an event.
- Any adverse event which compromises some aspect of computer or network security.
- An occurrence in a system that is relevant to the security of the system (event).

Why to Have Incident Response Systems?

- Rising number of threats in the cyberspace.

- Strong need for instituting incident response management systems in organization.

- Cyber attacks frequently cause the compromise of personal and business data.

- Real incidents involving viruses, worms, Trojan Horses, Spyware and other forms of Malicious Code.

Incident Response Team Work, Capabilities and Structure

- ✓An active coordination and management role needs to be created.
- ✓ The incident response team needs to be formed.
- ✓Staffing the incident response team is a tricky issue.
- ✓Team success is about skills, competencies, capabilities, and training.
- ✓Haphazard teams with inadequate skills will not work.

Incident Classification (High-Low Risk)

- High priority Incidents

  Malicious code Attack

- Medium priority Incidents

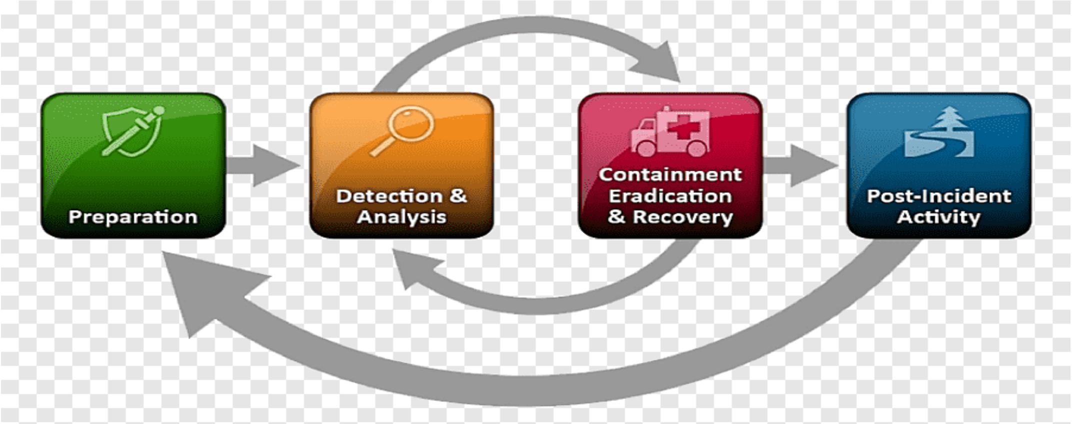
  Password Cracking Attack

- Low priority Incidents

  Probes and Network Scanning

Incident Response Life Cycle

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned



Preparation

- Establish incident response policies, roles, and responsibilities.
- Implement security measures like firewalls, intrusion detection systems (IDS), and antivirus solutions.
- Train employees on recognizing security threats and reporting incidents.

Identification

- Detect and recognize potential security incidents, such as unauthorized access, malware infections, or data breaches.

- Use monitoring tools (e.g., SIEM, IDS) to analyze network traffic and detect anomalies.

- Classify the incident's severity, type, and scope.

Containment

- Take immediate actions to prevent the incident from causing further harm. For example, isolating compromised systems or blocking malicious traffic.

- Short-term containment focuses on stopping the attack in progress, while long-term containment ensures systems are protected before being returned to normal operation.

Eradication

- Remove the root cause of the incident (e.g., deleting malware, closing security vulnerabilities).

- Identify all affected systems, ensuring no remnants of the threat remain.

Recovery

- Restore normal operations by bringing systems back online and ensuring they function properly and securely.

- Test systems to verify that they are free from any threats and vulnerabilities.

- Apply patches or updates to fix the security issues that caused the incident.

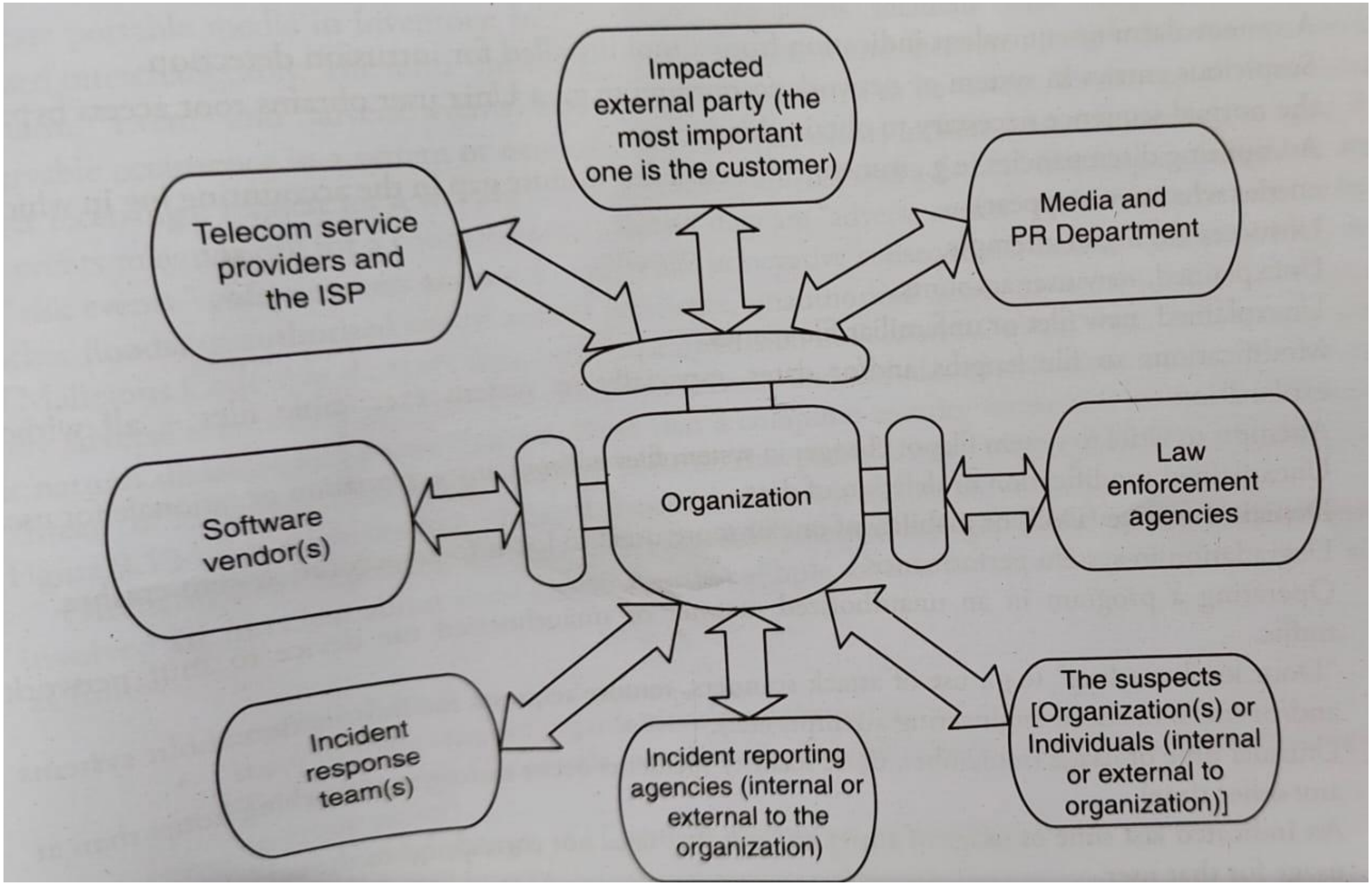
Lessons Learned

- Conduct a post-incident analysis to understand what happened, how it was handled, and what can be improved.

- Document the incident and the response to refine the organization’s security policies and procedures.

- Share findings with relevant stakeholders and update the incident response plan if necessary.

Incident Related Communication


Impacted external party (the most important one is the customer)
Telecom service providers and the ISP
Media and PR Department
Software vendor(s)
Organization
Law enforcement agencies
Incident response team(s)
Incident reporting agencies (internal or external to the organization)
The suspects [Organization(s) or Individuals (internal or external to organization)]

Steps for Incident Handling Process

- Identification
- Incident recording
- Initial response
- Communicating the incident
- Containment
- Formulating a incident response strategy
- Incident classification
- Incident investigation
- Data collection
- Forensic analysis
- Evidence protection
- Notify external agencies
- Eradication
- System recovery
- Incident documentation
- Incident damage and cost analysis
- Review and update the response policies
- Training awareness

Benefits of Incident Response Systems

1.Organization has the ability for responding to incidents systematically so that the appropriate steps are taken.

2. There is a provision for helping personnel to recover quickly and efficiently from security incidents, minimizing loss or theft of information and disruption of services. This results in timely resolution of incidents, resulting in reduced business impact.

3. Being able to use the information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data.

4. The ability to deal properly with legal issues that may arise during incidents.

5. Improved user satisfaction.

6. More efficient utilization of service desk and other staff .

7. Enhanced ability to measure and monitor IT performance relative to SLAs.

8. Better data to support executive decisions regarding service quality.

9. Improved ability to track incidents and service requests efficiently.

10. Proactive identification of process enhancements.

Benefits of Incident Response Systems

11. A systematically installed incident handling system makes it imperative for organization to carry out a root cause analysis of the incidents that have occurred.

12. It also helps to study if there is a “trend” and “pattern” in the cybersecurity incidents that have taken place.

13. Lessons learned from meetings provide other benefits.

14. Reports from these meetings are good material for training new team members.

15. Information regarding an incident may be recorded in several places.

16. Organizations should deploy centralized logging servers and configure devices to send duplicates of their log entries.

17. A system enforces recording of the information with regard to an incident.

18. Incident handlers benefit from this practice because they have the pertinent log entries available together.

19. Use of checklists helps to harmonize the incident response analysis

Media and Asset Protection: Best Practices for Organizations

- "Information asset": A definable piece of information stored in any manner that is recognized as "valuable" to the organization.

- Data breaches take place when criminals perceive "value" to the data/information stored on the media or see a particular information asset as valuable.

- **All data breach incidents may not necessarily involve only network attacks; even physical media can get stolen and crimes happen.**

- It is imperative to have local encryption for hard disks and any other media that are believed to store critical information.

- Even when the information is classified and a scheme is deployed for information asset protection, it is of no use without an effective access management system.

- Managing the access to organization's information assets is of paramount importance.

Media and Asset Protection

- “Access” is the ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.

- Access management is the process for managing individual and group authorization to read, create, modify or transfer data, and to perform specific functions or transactions.

- Access management framework is the consolidation of all access management standards, requirements and resource references to incorporate business unit best practices in a single document.

- Employees in the organization are committed to information protection and are responsible for classifying and protecting information that has value to the organization, its employees and the customers, suppliers, business partners and others with whom the organization does business.

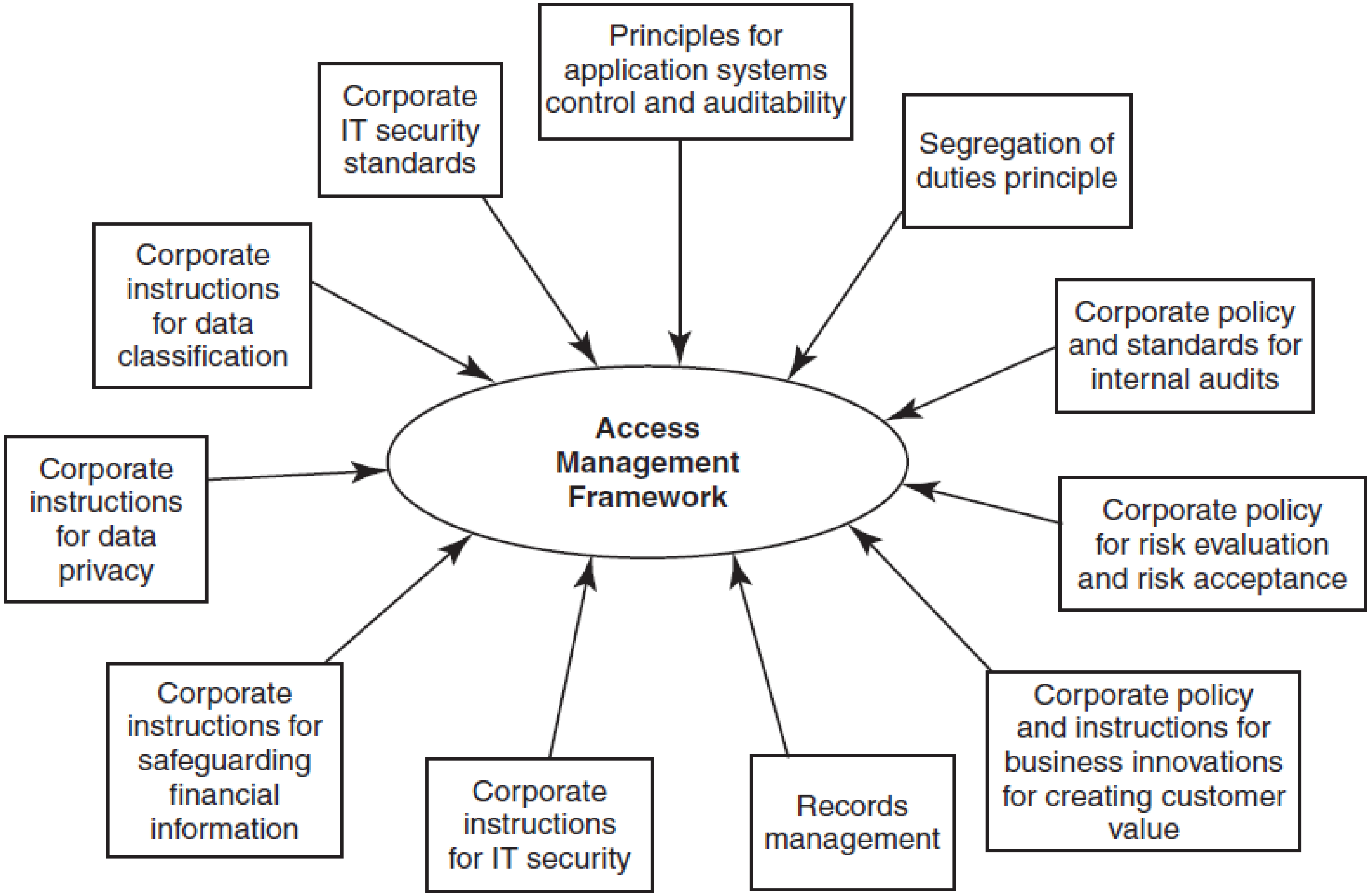
Access management framework

1. **What:** Identification of data and functions that need to be protected.

2. **Who:** Determination of who should have access to specific data and/or functions and why they should have access (authorization criteria).

3. **How:** Definition of the specific method to request, evaluate, approve (or reject) and implement access authorization.

Access management framework



Access Management Framework

Corporate IT security standards

Principles for application systems control and auditability

Segregation of duties principle

Corporate instructions for data classification

Corporate policy and standards for internal audits

Corporate instructions for data privacy

Corporate policy for risk evaluation and risk acceptance

Corporate instructions for safeguarding financial information

Corporate instructions for IT security

Records management

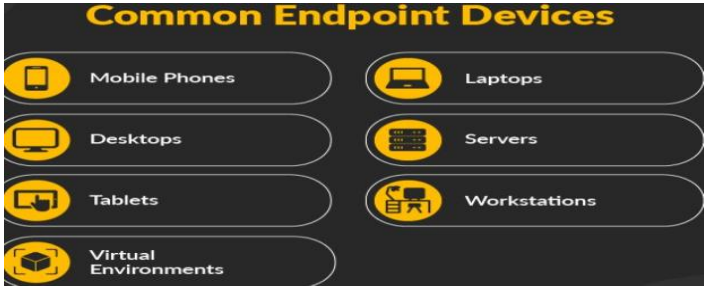
Corporate policy and instructions for business innovations for creating customer value

Figure 5 | Access management framework – key elements.

Importance of Endpoint Security in Organizations

- An “endpoint” is an individual computer system or device that acts as a network client and serves as a workstation or personal computing device.

- Common endpoints are laptops, desktops and personal computing devices including hand-held devices that can connect into the network.



Common Endpoint Devices

Mobile Phones

Laptops

Desktops

Servers

Tablets

Workstations

Virtual Environments

- Securing the endpoints is essential to protect assets.

- Organizations that do not have any form of endpoint security, have their corporate networks and data potentially exposed to hackers and criminals who can access sensitive information from unprotected access points.

Importance of Endpoint Security in Organizations

- People who are out of a job are found to steal confidential company information with them either on DVD or using USB drives.

- Security risks from hand-held devices (such as iPods, USB devices, Smartphones, etc.) have dramatically increased the risk of intentional and unintentional data leaks and other malicious activity.

- The use of portable storage devices poses a huge security risk to networks at the endpoints.

- Moreover, securing these endpoints has become a major area of concern for IT security implementers in corporate as well as small and medium enterprises.

Importance of Endpoint Security in Organizations

- Web-based applications are more prone to security threats.
- E-Mails have become the most common method or primary means of communication for almost all organizations and individuals.
- Most people are not careful when sending information through E-Mails.
- Highly confidential information inside the E-Mail text and/or sent as attachments results in possible breach of confidential data through E-Mail system.

Organizations can take a number of actions:

- Devices can be tested for security compliance, and devices that fail compliance testing should be quarantined.

- Users of those devices should be provided with directions and resources for updating the device with the necessary patches and security settings.

- **It is to be remembered that endpoint compliance includes both kinds of devices:**

(1) Devices that are under the control of the organization (corporate desktops and laptops)

(2) External endpoints that are not under the organization’s direct control.

Summary

- **Cost of Cybercrimes and IPR Issues**
- **Web Threats**
- **Security and Privacy Implications - Social Media Marketing**
- **Social Computing and the Challenges**
- **Protecting People’s Privacy**
- **Organizational Guidelines**
- **Incident Handling**
- **Media and Asset Protection**
- **Importance of End Point Security**