UNIT-5

CYBER SECURITY: ORGANIZATIONAL IMPLICATIONS

- Introduction
- Cost of Cyber Crimes
- IPR Issues
- Web Threats for Organizations
- Security and Privacy Implications
- Social Media Marketing: Security Risks
- Perils for Organizations
- Social Computing and associated challenges for organizations.

Organizational Implications-Introduction

In the 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.

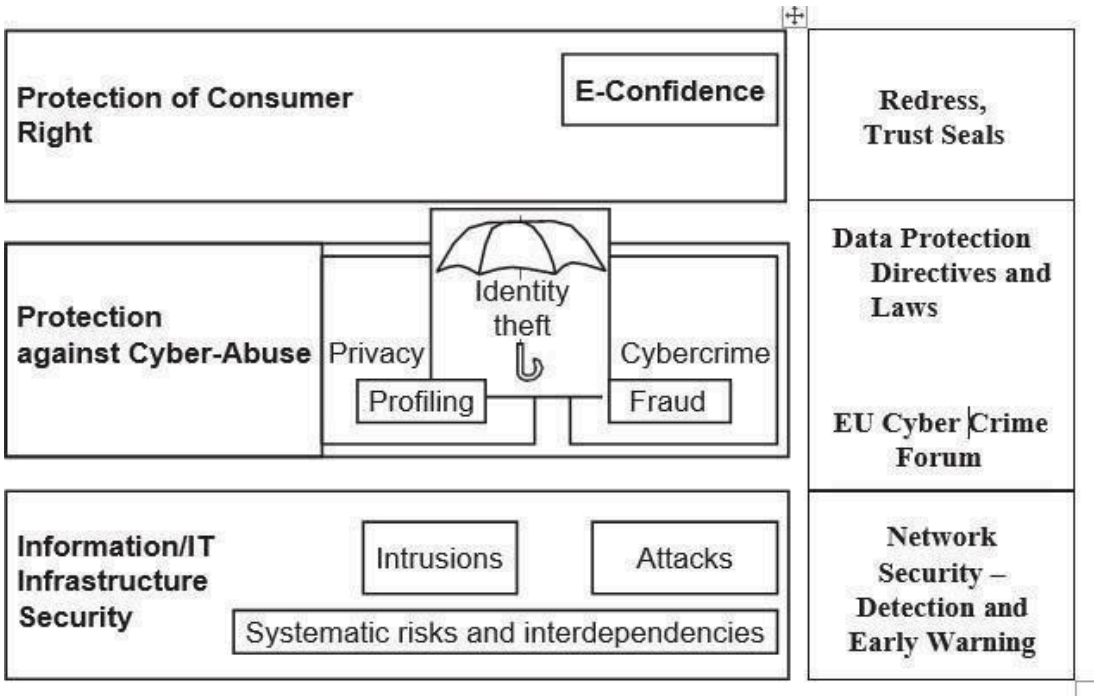


Fig: A cyber security perspective. EU is the European Union.

PI is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual.

Most information the organization collects about an individual is likely to come under "PI" category if it can be attributed to an individual. For an example, PI is an individual's first name or

first initial and last name in combination with 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 codes or password that would permit access to an individual's financial account.
4. Home address or E-Mail address.
5. Medical or health information.

An insider threat is defined as "the misuse or destruction of sensitive or confidential information, as well as IT equipment that houses this data by employees, contractors and other 'trusted' individuals."

Insider threats are caused by human actions such as mistakes, negligence, reckless behavior, theft, fraud and even sabotage. There are three types of "insiders" such as:

1. A malicious insider is motivated to adversely impact an organization through a range of actions that compromise information confidentiality, integrity and/or availability.
2. A careless insider can bring about a data compromise not by any bad intention but simply by being careless due to an accident, mistake or plain negligence.
3. A tricked insider is a person who is "tricked" into or led to providing sensitive or private company data by people who are not truthful about their identity or purpose via "pretexting" (known as social engineering).

- **Insider Attack Example 1: Heartland Payment System Fraud**

  A case in point is the infamous "Heartland Payment System Fraud" that was uncovered in January 2010. This incident brings out the glaring point about seriousness of "insider attacks. In this case, the concerned organization suffered a serious blow through nearly 100 million credit cards compromised from at least 650 financial services companies. When a card is used to make a purchase, the card information is trans- mitted through a payment network.

- **Insider Attack Example 2: Blue Shield Blue Cross (BCBS)**

  Yet another incidence is the Blue Cross Blue Shield (BCBS) Data Breach in October 2009 the theft of 57 hard drives from a BlueCross BlueShield of Tennessee training facility puts the private information of approximately 500,000 customers at risk in at least 32 states. The two lessons to be learnt from this are:

  1. Physical security is very important.
  2. Insider threats cannot be ignored.

What makes matters worse is that the groups/agencies/entities connected with cybercrimes are all linked. There is certainly a paradigm shift in computing and work practices; with workforce mobility, virtual teams, social computing media, cloud computing services being offered, sharp rise is noticed in business process outsourcing (BPO) services, etc. to name a few.

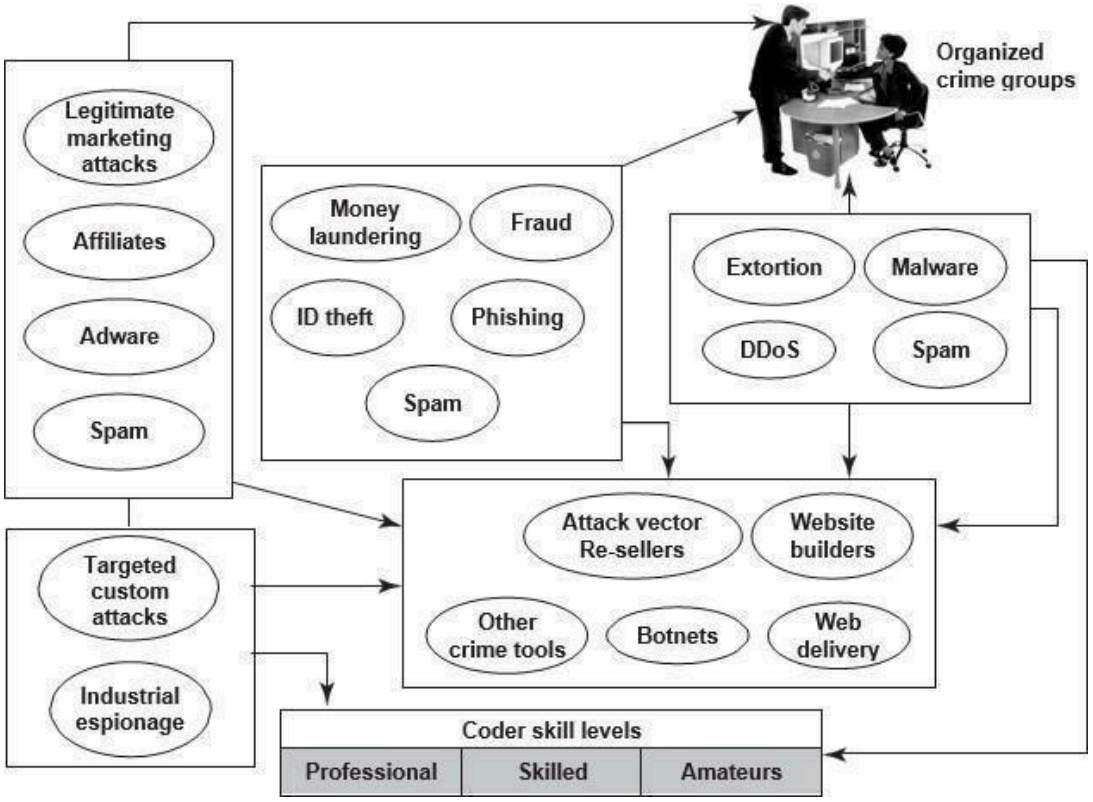


Fig: Cybercrimes – the flow and connections.

A key message from this discussion is that cybercrimes do not happen on their own or in isolation. Cybercrimes take place due to weakness of cybersecurity practices and "privacy" which may get impacted when cybercrimes happen.

Privacy has following four key dimensions:

1. **Informational/data privacy:** It is about data protection, and the users' rights to determine how, when and to what extent information about them is communicated to other parties.
2. **Personal privacy:** It is about content filtering and other mechanisms to ensure that the end-users are not exposed to whatever violates their moral senses.
3. **Communication privacy:** This is as in networks, where encryption of data being transmitted is important.
4. **Territorial privacy:** It is about protecting users' property for example, the user devices from being invaded by undesired content such as SMS or E-Mail/Spam messages. The paradigm shift in computing brings many challenges for organizations; some such key challenges are described here.

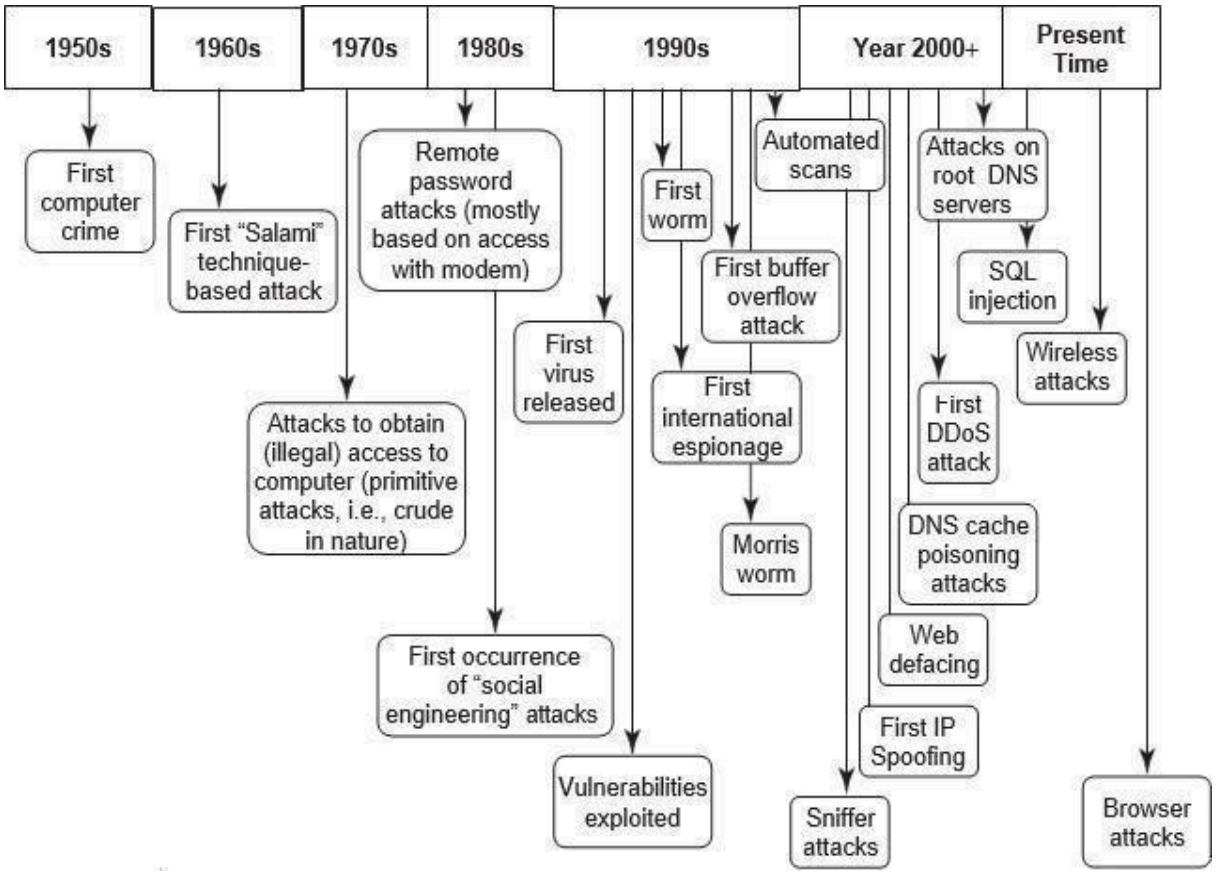


Fig: Security threats – paradigm shift.

The key challenges from emerging new information threats to organizations are as follows:

1. **Industrial espionage:** There are several tools available for web administrators to monitor and track the various pages and objects that are accessed on their website.
2. **IP-based blocking:** This process is often used for blocking the access of specific IP addresses and/or domain names.
3. **IP-based "cloaking":** Businesses are global in nature and economies are interconnected.
4. **Cyberterrorism:** "Cyberterrorism" refers to the direct intervention of a threat source toward your organization's website.

Confidential information leakage: "Insider attacks" are the worst ones. Typically, an organization is protected from external threats by your firewall and antivirus solutions

cybercrimes cost a lot to organizations.

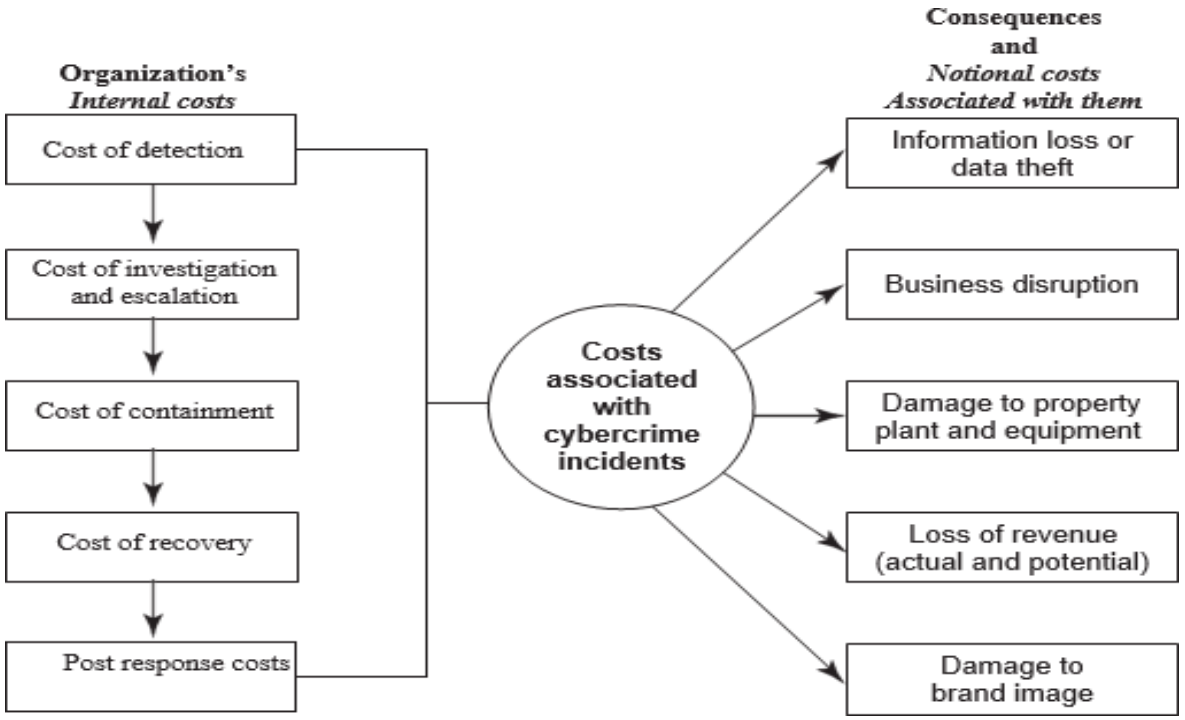


Fig: Cost of cybercrimes.

When a cybercrime incidence occurs, there are a number of internal costs associated with it for organizations and there are organizational impacts as well.

Detection and recovery constitute a very large percentage of internal costs. This is supported by a benchmark study conducted by Ponemon Institute USA carried out with the sample of 45 organizations representing more than 10 sectors and each with a head count of at least 500 employees.

- **Organizations have Internal Costs Associated with Cyber security Incidents**

The internal costs typically involve people costs, overhead costs and productivity losses. The internal costs, in order from largest to the lowest and that has been supported by the benchmark study mentioned:

1. Detection costs.(25%)
2. Recovery costs.(21%)
3. Post response costs.(19%)

4. Investigation costs.(14%)
5. Costs of escalation and incident management.(12%)
6. Cost of containment.(9%)

- **The consequences of cybercrimes and their associated costs, mentioned**
  1. Information loss/data theft.(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%)
- **The impact on organizations by various cyber crimes**
  1. Virus,worms and Trojans-100%
  2. Malwares-80%
  3. Botnets-73%
  4. Web based attacks-53%
  5. Phishing and Social engineering-47%
  6. Stolen devices-36%
  7. Malicious insiders-29%
  8. Malicious code-27%
- **Average days taken to resolve cyber Attacks**

1. Attacks by Malicious insiders-42 days
2. Malicious code-39 days
3. Web based attacks-19 days
4. Data lost due to stolen devices-10 days
5. Phishing and social engineering attacks-9 days
6. Virus,worms,and trojans-2.5 days
7. Malware-2 days
8. Botnets- 2 days

- **There are many new endpoints in today's complex networks; they include hand-held devices.**

  Again, there are lessons to learn:

  1. **Endpoint protection:** It is an often-ignored area but it is IP-based printers, although they are passive devices, are also one of the endpoints.
  2. **Secure coding:** These practices are important because they are a good mitigation control to protect organizations from "Malicious Code" inside business applications.
  3. **HR checks:** These are important prior to employment as well as after employment.
  4. **Access controls:** These are always important, for example, shared IDs and shared laptops are dangerous.

5. **Importance of security governance:** It cannot be ignored policies, procedures and their effective implementation cannot be over-emphasized.

- **Organizational Implications of Software Piracy**

Use of pirated software is a major risk area for organizations.

From a legal standpoint, software piracy is an IPR violation crime. Use of pirated software increases serious threats and risks of cybercrime and computer security when it comes to legal liability.

The most often quoted reasons by employees, for use of pirated software, are as follows:

1. Pirated software is cheaper and more readily available.
2. Many others use pirated software anyways.
3. Latest versions are available faster when pirated software is used.

Web Threats for Organizations: The Evils and Perils

Internet and the Web is the way of working today in the interconnected digital economy. More and more business applications are web based, especially with the growing adoption of cloud computing.

- **Overview of Web Threats to Organizations**

The Internet has engulfed us! 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.

IT managers must also find a balance between allowing reasonable personal Internet use at work and maintaining office work productivity and work concentration in the office.

- **Employee Time Wasted on Internet Surfing**

This is a very sensitive topic indeed, especially in organizations that claim to have a "liberal culture." Some managers believe that it is crucial in today's business world to have the finger on the pulse of your employees.

People seem to spend approximately 45-60 minutes each working day on personal web surfing at work.

- **Enforcing Policy Usage in the Organization**

An organization has various types of policies. A security policy is a statement produced by the senior management of an organization, or by a selected policy board or committee to dictate what type of role security plays within the organization.

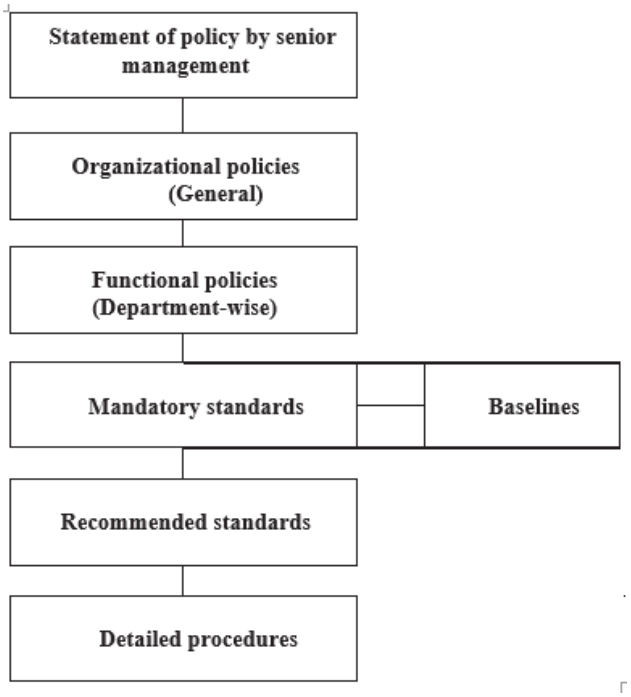


Fig: Policy hierarchy chart.

- **Monitoring and Controlling Employees' Internet Surfing**

A powerful deterrent can be created through effective monitoring and reporting of employees' Internet surfing.

Even organizations with restrictive policies can justify a degree of relaxation; for example, allowing employees to access personal sites only during the lunch hour or during specified hours.

- **Keeping Security Patches and Virus Signatures Up to Date**

Updating security patches and virus signatures have now become a reality of life, a necessary activity for safety in the cyberworld! Keeping security systems up to date with security signatures, software patches, etc. is almost a nightmare for management.

- **Surviving in the Era of Legal Risks**

As website galore, most organizations get worried about employees visiting inappropriate or offensive websites. We mentioned about Children's Online Privacy Protection.

Serious legal liabilities arise for businesses from employee's misuse/inappropriate use of the Internet.

- **Bandwidth Wastage Issues**

Today's applications are bandwidth hungry; there is an increasing image content in messages and that too, involving transmission of high-resolution images.

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

- **Mobile Workers Pose Security Challenges**

  Use of mobile handset devices in cybercrimes. Most mobile communication devices for example, the personal digital assistants has raised security concerns with their use. Mobile workers use those devices to connect with their company networks when they move. So the organizations cannot protect the remote user system as a result workforce remains unprotected. We need tools to extend web protection and filtering to remote users, including policy enforcement

- **Challenges in Controlling Access to Web Applications**

  Today, a large number of organizations' applications are web based. There will be more in the future as the Internet offers a wide range of online applications, from webmail or through social networking to sophisticated business applications. Employees use personal mail id to send business sensitive information (BSI) for valid or other reasons. It leads to data security breach. The organizations need to decide what type of access to provide to employees.

- **The Bane of Malware**

  Many websites contain malware. Such websites are a growing security threat. Although most organizations are doing a good job of blocking sites declared dangerous, cyber attackers, too, are learning. Criminals change their techniques rapidly to avoid detection.

- **The Need for Protecting Multiple Offices and Locations**

  Delivery from multi-locations and teams collaborating from multi-locations to deliver a single project are a common working scenario today. Most large organizations have several offices at multiple locations. In such scenario Internet-based host service is best idea to protect many locations.

Security and privacy implications from cloud computing

Cloud computing is one of the top 10 Cyber Threats to organizations. There are data privacy risks through cloud computing. Organizations should think about privacy scenarios in terms of "user spheres". There are three kinds of spheres and their characteristics:

1. **User sphere:** Here data is stored on users' desktops, PCs, laptops, mobile phones, Radio Frequency Identification (RFID) chips, etc. Organization's responsibility is to provide access to users and monitor that access to ensure misuse does not happen.
2. **Recipient sphere:** Here, data lies with recipients: servers and databases of network providers, service providers or other parties with whom data recipient shares data. Organizations responsibility is to minimize users privacy risk by ensuring unwanted exposure of personal data of users does not happen

3. **Joint sphere:** Here data lies with web service provider's servers and databases. This is the in between sphere where it is not clear to whom does the data belong. Organization responsibility is to provide users some control over access to themselves and to minimize users futures privacy risk.

Social Media Marketing: Security Risks and Perils for Organizations

Social media marketing has become dominant in the industry. According to fall 2009 survey by marketing professionals; usage of social media sites by large business-to-business (B2B) organizations shows the following:

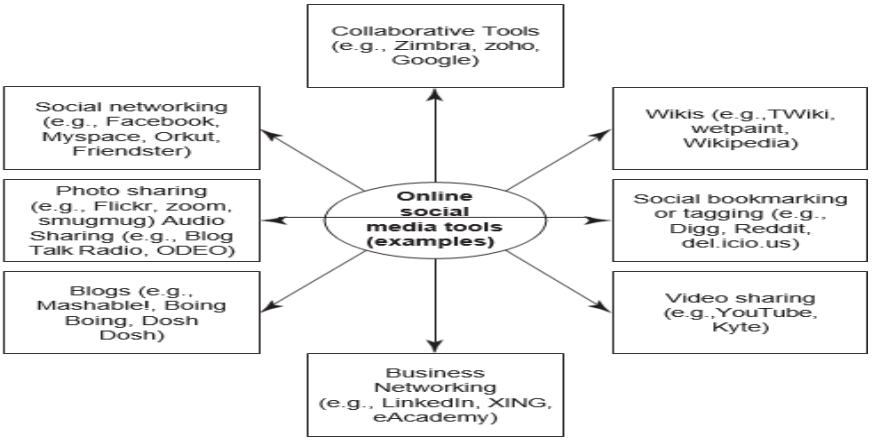


FIG: Social Media Marketing Tools

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. My Space is used by 6% of the organizations.

Although the use of social media marketing site is rampant, there is a problem related to "social computing" or "social media marketing" – the problem of privacy threats. Exposures to sensitive PI and confidential business information are possible if due care is not taken by organizations while using the mode of "social media marketing."

- **Understanding Social Media Marketing**

Most professionals today use social technologies for business purposes. Most common usage include: marketing, internal collaboration and learning, customer service and support, sales, human resources, strategic planning, product development.

Following are the most typical reasons why organizations use social media marketing to promote their products and services:

1. To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertising fees.
2. To increase traffic to their website coming from other social media websites by using Blogs

and social and business-networking. Companies believe that this, in turn, may increase their "page rank" resulting in increased traffic from leading search engines.

3. To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertising campaign.
4. To build credibility by participating in relevant product promotion forums and responding to potential customers' questions immediately.
5. To collect potential customer profiles. Social media sites have information such asuser profile data, which can be used to target a specific set of users for advertising

There are other tools too that organizations use; industry practices indicate the following:

1. Twitter is used with higher priority to reach out to maximum marketers in the technology space and monitor the space.
2. Professional networking tool LinkedIn is used to connect with and create a communityof top executives from the Fortune 500.
3. Facebook as the social group or social community tool is used to drive more traffic to Websense website and increase awareness about Websense.
4. YouTube (the video capability tool to run demonstrations of products/services, etc.) is used to increase the brand awareness and create a presence for corporate videos.
5. Wikipedia is also used for brand building and driving traffic.

There are conflicts views about social media marketing some people in IT say the expensive and careless use of it. Some illustrate the advantages of it with proper control of Security risk

Organizational Guidelines for Internet Usage, Safe Computing Guidelines and Computer Usage Policy

IT managers need to recognize the need for protecting their companies identity when online. Each time an employee accesses the internet, the individual may leak pieces of information to competitors, hackers and online predators. Anonymizer mitigates these threats with their identity protection and information assurance solutions. In view of the cyberthreats, it becomes important for organization to develop safe computing guideline. Therefore, first we will start the computer usage policy.

Developing and organizational policy for computer usage

At basic level, a "Computer Usage Policy" should address the following elements

Mission Statement

First, policy should briefly but meaningfully state the organization's mission because policies must support the

mission of the organization.

Example: In public library, assuming that the library makes provisions for access to the internet, the mission statement could read like:

"<XYZ> library system provides the public of so and so area <ABC> with excellent service and convenient access to resources for their educational, informational and recreational needs"

Introduction

It should explain what the policy document is about and what it contains as well as the scope of the policy.

Internet Safety

The most important section. Assuming the same example, in public library

<XYZ> library addresses the following internet safety issues through its Acceptable Use Agreement, Parental Permission Form and use of technology protection measures on library computers. Policy could address the,

1. Access by minors to inappropriate matter on the Internet.
2. Safety and security of minors during usage of email, chat rooms
3. Unauthorized access, including hacking and other lawful activities by minor online
4. Unauthorized disclosure, use and dissemination of personal identification information regarding minors.
5. Measures designed to restrict minors access to materials harmful to minors.

Confidentiality

It constitutes a very important section in a policy about safe computing. Library shall treat data stored on computers as confidential.

Disciplinary action for Privacy Violation and Disclaimer

The last two important sections of safe computing policy. Those who violate the computer usage policy may lose library privileges. Violations of policy will be subjected to disciplinary action.

Disclaimer

Internet is a global electronic network. There is no control over users or website content.

UNIT-5

Cybersecurity: Organizational Implications

→ Best Practices with Social media Marketing Tools.

1) "Establish Social Media policy": Use of personal blogging for work related matters should be monitoried & minimized.

↳ Use of policies and implementation of policy-based procedures are always essential.

↳ Once the policy has created, employers should communicate it to employees & should enforce its implementation through continuous monitoring.

↳ Organizations need to educate their employees about the risk associated with the use of online social media tools

↳ It is worth of exploring appointment of a social media expert within the company so that he can serve as a permanent contact for employees for their questions on social media marketing tool usage.

2) Establish firm processes based on the policy:

↳ Network administrators need to remain up to date about the most recent risks on the web.

↳ There is a strong need to establish firm processes that are systematically linked to daily workflows.

↳ Example IT Admin should ensure that the latest security updates are downloaded & to identify Network attacks in time to avoid them.

3) Need based access policy establishment.

↳ With this risk of information falling into wrong hands through unauthorized channels is reduced.

↳ It helps to control & monitor access to critical data, and to track such access at anytime.

↳ policies should not be treated as one-time activity they must be updated & adapt them to changing circumstances.

4) Blocking the infected websites ~~is done~~

↳ URL filters allow organizations to block access to known malware & phishing websites.

↳ Access blocking can also be applied to any other suspicious site on Internet.

↳ The filter function should be kept up to date by maintaing so-called black- and white listed websites.

5) Use of firewalls.

↳ Firewalls helps organization keep their security technology up to date,

↳ Some fire walls provide a comprehensive analysis of all data traffic, which make it possible to monitor the type of data traffic, the websites from which it is coming, to know the web patterns & peer to-peer applicati-ons to encrypted data traffic in SSL (Secure Socket Layer) tunnel.

6) Protection against vulnerability: It is possible by carefully planning vulnerability scanning & penetration testing.

↳ An Intrusion prevention system (IPS) serves as a protective barrier to the corporate Network by preventing automatically ~~from~~ ~~too~~ attacks by worms, viruses & other malwares.

(7) Define Access to business Applications : Define need based access to business Applications that reside on corporate Networks as well as on the external sites.

↳ Example Ex of SSL VPN portal — VPN is virtual private N/w a tunnel within the internet.

↳ A strong level authentication via single sign-on for the user. As a result single login makes it possible for users to access only the Network area & services for which they are authorized.

(8) Securing the Intranets: They are not spared by cyberattackers.

↳ Intranet of every company consists highly sensitive information pretaining to the business are involved. They should be isolated from rest of internal N/w by using ~~its~~ the firewalls to segment the Intranet.

↳ this enables segregation of departmental intranets.

↳ Ex: a company can seperate departments such as finance or accounting from the rest of the penetrating critical segments of the corporate N/w.

↳ this can be done by DMZ Network (demilitarized Zone Network).

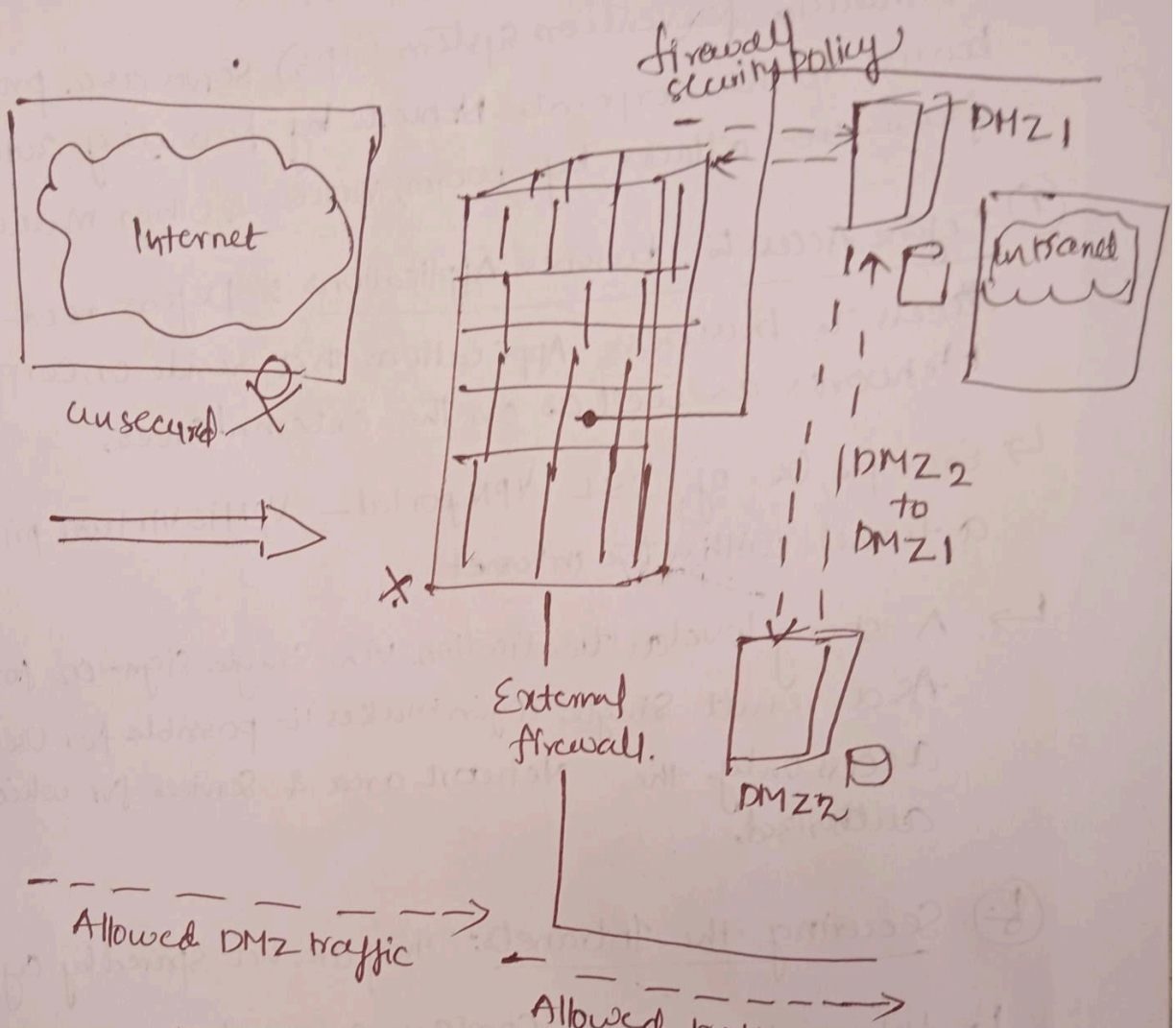


FIG: Firewall with DMZ Network

⑨ Include Mobile devices in security policy:

↳ It is common for users to Navigate from social webservices with mobile devices such as laptops, PDA & smart phones.

↳ The same devices are used to log into the corporate N/w.

↳ The corporate security department, therefore needs to include mobile devices in the securing policies by checking login device for required security settings & presence of securing-relevant s/w packages.

(10) Use of Centralized Management: Administrators can manage, monitor and configure the entire N/w and all devices using a single management console.

↳ They can also monitor user activities on the N/w by viewing reports.

Ex: System administrator will be able to know who has accessed which data at what time.

↳ this allows preventing attacks more efficiently & provide more protection for corporate Applications at risk.

* Organizational best practices are listed below

1. Organization-wide information systems security policy
2. Configuration/change control and mangement
3. Risk assesment & management
4. Standardized s/w configurations that satisfy the information system security policy
5. Security awareness and training
6. Contingency planning, continuity of operations & disaster recovery planning.
7. Certification and accrediation

→ Social Computing and the Associated challenges for organizations

- It is also known as "Web 2.0"
- It empowers people to use web-based public products and services.
- It helps thousands of people across the globle to support their work, health, learning, getting entert

-ained and citizienship tasks in a number of innovative ways.

↳ In this process, a lot of information gets exchanged & some of that could be confidential, personally identifiable information (PII)/SPI etc., This would be gold mine for the cyber criminals.

↳ Getting too used to readily available information, people may get into the mode of not questioning the accuracy & reliability of information that they readily get on the internet.

↳ with social computing, there are new threats emerging, those threats relate to security, safety & privacy.

* Technical terms *

↳ Various types of mobile workers/remote workers.

1. ~~Tied~~ Tethered/remote workers: An employee who remains at a single point of work, but is remote to the central company system.

   Ex: Homeworkers, telecottages, branch workers.

2. Roaming user: An employee works in an environment (eg: warehouses, shopfloor etc.) or in multiple areas (eg: meeting rooms)

3. Nomad: Employees requiring solutions in hotel

modem use is still prevalent, along with wireless technologies & devices

4. Road warrior: This is the ultimate mobile user, such a remote worker spends little time in the office, however he/she requires regular access to data and collaborative functionality while on the move, in transit or in hotels

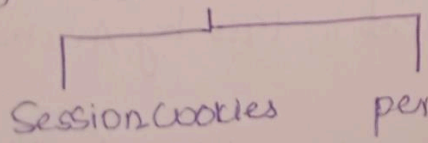
Ex: Sales & field forces.

↳ Cookies

↳ A piece of information that get passed to your browser by a server on the Internet.

↳ They are stored on the hard drive and are returned to server when requested.

↳ Cookies



↳ 1) Session cookie is also called "transient cookie" which lasts only for the duration of the internet session.

↳ 2) persistent cookie also called stored cookie

↳ It gets stored on the user's hard drive until it expires or the user deletes the cookie.

↳ In 1994, Netscape created cookies as a special browser feature. It did so to make Internet browser's life easier while Surfing on the web.

↳ Proactive Vs. Reactive Approach to security

* Proactive approaches are the measures taken with the aim to thwart host-based or N/w based attacks from successfully compromising systems.
  ↳ This help prevent future businesss losses.
* Reactive approaches used after it has been discov-ered that some of organization's systems have been compromised by an intruder or attack program

↳ Protecting your Online privacy

↳ "Dataveillance" was coined in 1988 by Australian privacy expert clarke.
↳ It is about monitoring people no through their actions but through data trails about them.
↳ "personal Dataveillance" → Monitoring "identified individuals"
↳ "Mass Dataveillance" → monitoring of whole populations.
↳ The New method browser finger printing → to track you online. It can identify far more accurately than Cookie.
↳ It pull data about your browser, plug-in, systemfonts & OS.

Ex: Bank use this to prevent from frauds.

↳ Cookies & fair information practices to Avoid privacy Loss.

↳ IPPs (Information privacy principles) are set out general rules for organization to apply to build the content Use of cookies with regards privacy.

IPP1 — Collection: Manner & ~~plot~~ Purpose of collection of PI

IPP2 — Use & disclosure: Solicitation of PI from individual concerned.

IPP3 — Data quality: Solicitation of PI generally

IPP4 — Data security: Storage & security of PI

IPP5 — Openness: Information relating to records kept by record keeper.

IPP6 — Access & Correction: Access to record containing PI.

IPP7 — Identifiers: Alteration of records containing PI

IPP8 — Anonymity: Record-keep to check accuracy ~~etc~~. etc. of PI before use.

IPP9 — Transborder data flows: PI to be used only for relevant purposes.

IPP10 — Sensitive information: Limits on use of PI

IPP11 — Limited disclosure: Limits on the disclosure of PI.

———o——o——o———