CYBER SECURITY: ORGANIZATIONAL IMPLICATIONS

INTRODUCTION

COST OF CYBERCRIMES AND IPR ISSUES

WEB THREATS FOR ORGANIZATIONS

SECURITY AND PRIVACY IMPLICATIONS

SOCIAL MEDIA MARKETING: SECURITY RISKS AND PERILS FOR ORGANIZATIONS

SOCIAL COMPUTING AND THE ASSOCIATED CHALLENGES FOR ORGANIZATIONS.

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -

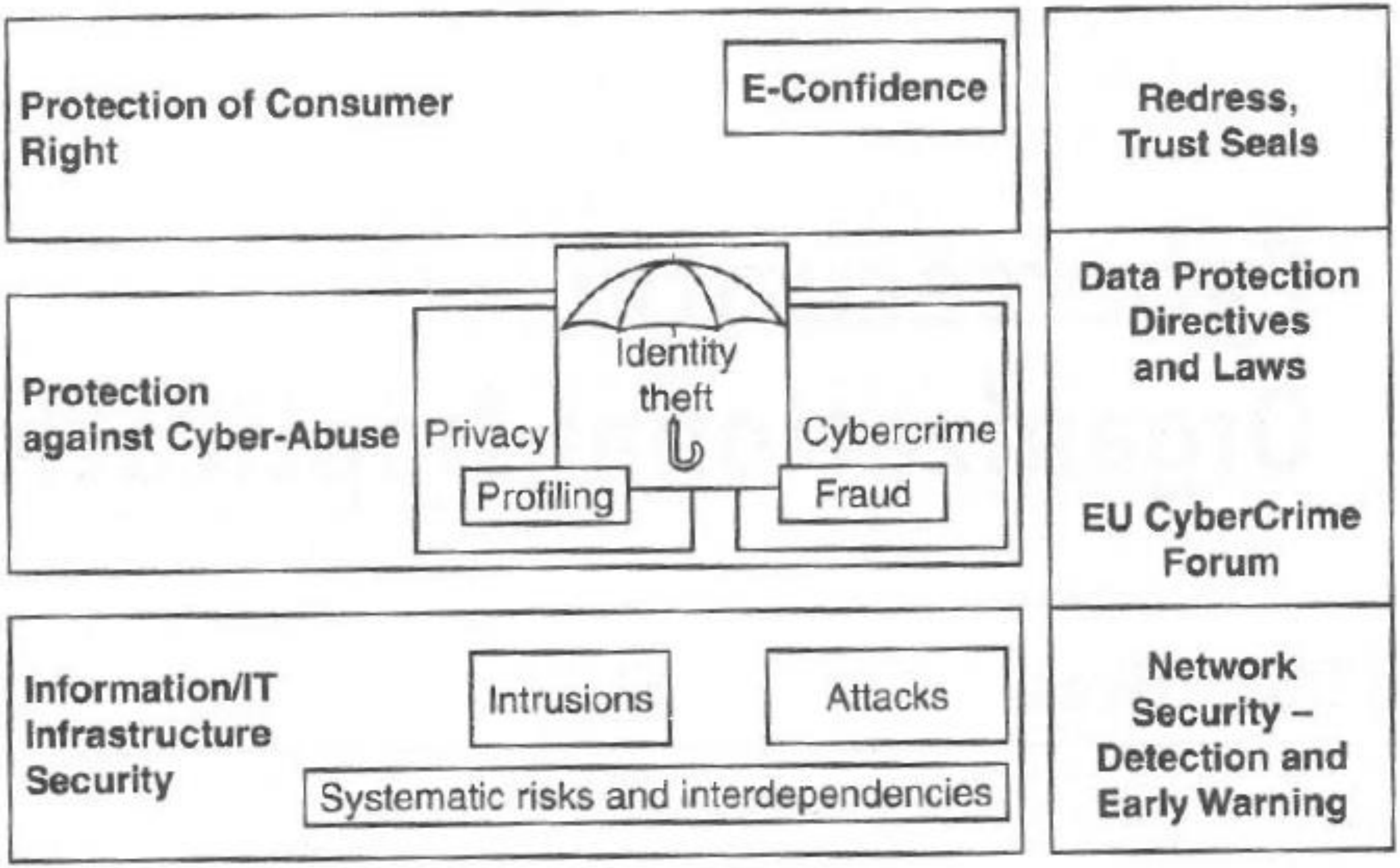
UNIT-5

INTRODUCTION

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- In the global environment with continuous network connectivity, the possibilities for cyber attacks can emanate from sources chat 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 incense scans from criminal groups.
- There are “security challenges with mobile workforce”
- Not to forget are the insider threats.
- A “security breach” is defined as unauthorized acquisition of data that comprimises security, confidentiality, or integrity of Personal Information(PI) maintained by us.
-

INTRODUCTION


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

A cybersecurity perspective. EU is the European Union.

INTRODUCTION

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- 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:
  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

INTRODUCTION

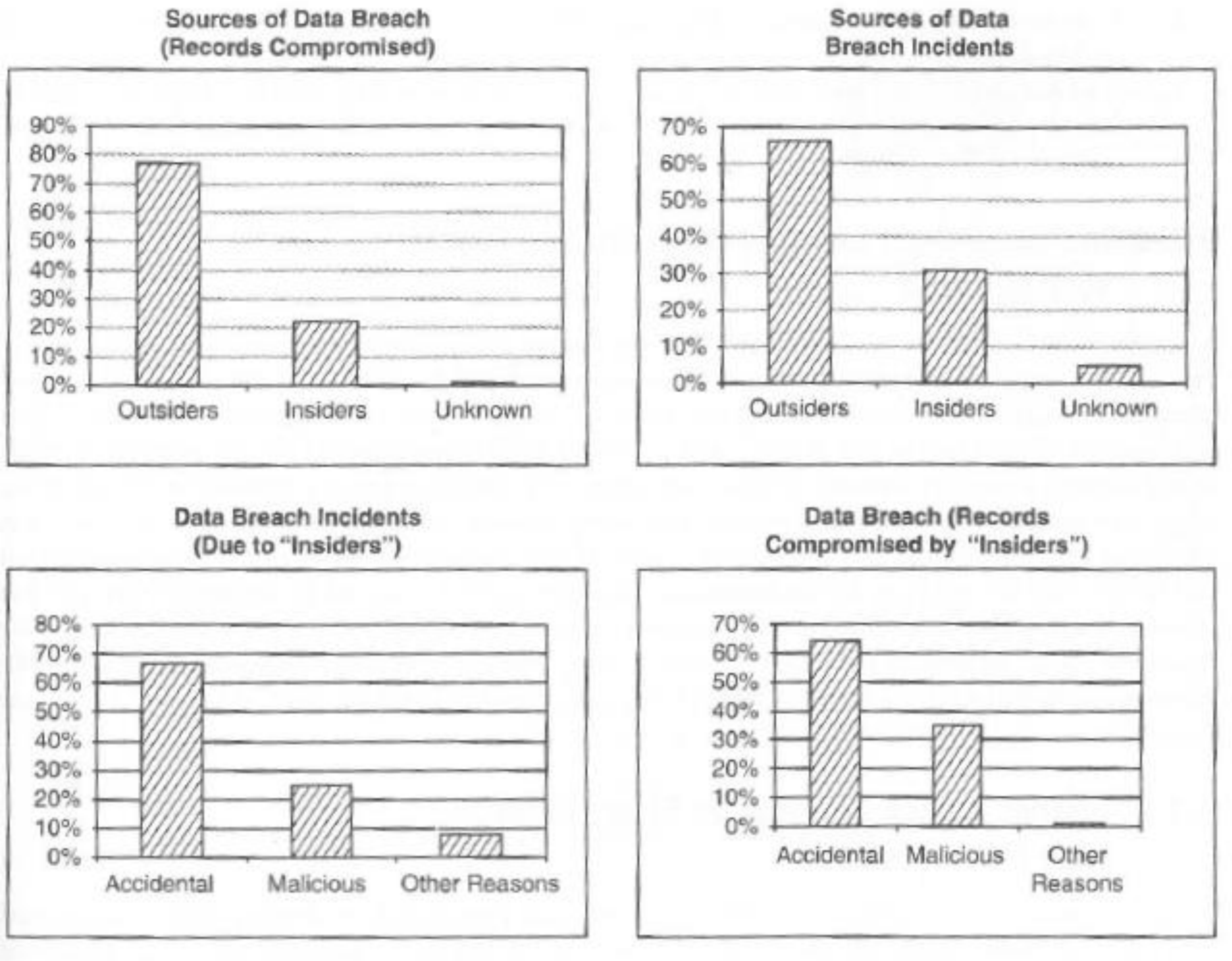


Fig: User Threat Scenario

INTRODUCTION

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- 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).

INTRODUCTION

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

Insider Attack Example-1 (Heartland Payment System Fraud)

- 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 transmitted through a payment network. In this case, a piece of malicious software (malware, i.e., a "keystroke logger") planted on the company's payment processing network, recorded payment card data as it was being sent for processing to Heartland by thousands of the company's retail clients.

Insider Attack Example-2 (Blue Shield Blue Cross)

- 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 hard drives containing 1.3 million audio files and 300,000 video files related to coordination of care and eligibility telephone calls from providers and members were reportedly stolen from a leased office. Three hard drives (3.5" x 10") were physically removed from server racks on computers inside data storage closet at a training center. Incidences such as these bring out glaring point about physical security weakness at organizations. The two lessons to be learnt from this are:
  - 1. Physical security is very important.
  - 2. Insider threats cannot be ignored.

INTRODUCTION

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- 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.
- Over a period of time, security threats to organizations have morphed from simple ones to very sophisticated ones
- The number of security attacks as well as their sophistication and variety rose from the 1980s and onward; this is in line with the sophistication of cybercriminals over a period of time.
- A key message is that cybercrimes do not happen on their own or in isolation. Cybercrimes take place due to weakness of cyber security practices and "privacy" which may get impacted when cybercrimes happen.

INTRODUCTION

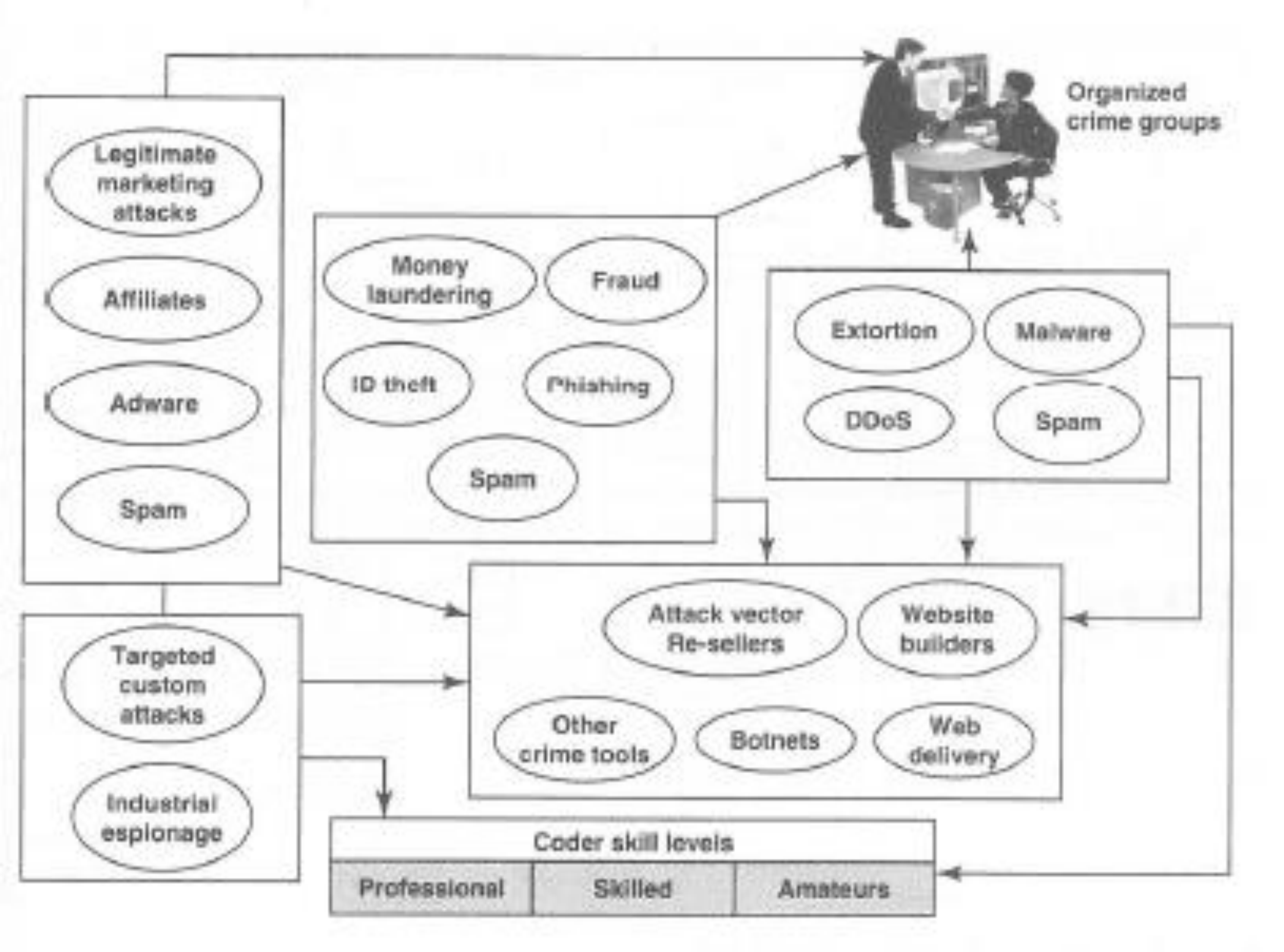


Fig: Cybercrimes – the flow of connections

INTRODUCTION

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- 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. The execution of this right may be based upon their knowledge about what the other party's intention is.
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.

INTRODUCTION

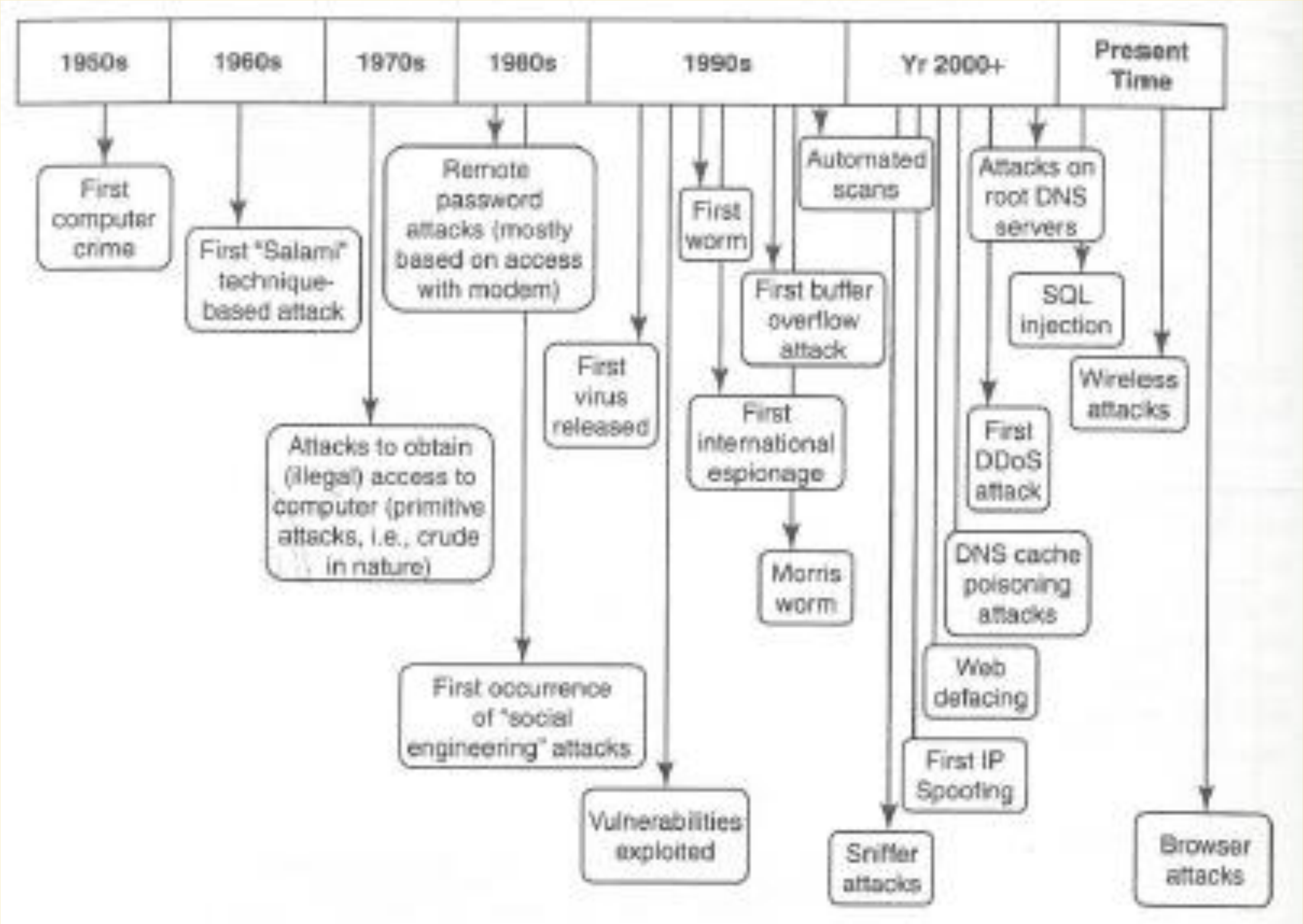

1950s
1960s
1970s
1980s
1990s
Yr 2000+
Present Time
First computer crime
First "Salami" technique-based attack
Remote password attacks (mostly based on access with modem)
Attacks to obtain (illegal) access to computer (primitive attacks, i.e., crude in nature)
First occurrence of "social engineering" attacks
First virus released
Vulnerabilities exploited
First worm
First international espionage
Morris worm
First buffer overflow attack
Automated scans
Sniffer attacks
First IP Spoofing
Web defacing
DNS cache poisoning attacks
First DDoS attack
Attacks on root DNS servers
SQL injection
Wireless attacks
Browser attacks

Fig: Security threats – Paradigm shift

INTRODUCTION

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

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. For example, suppose your competitor's networks, using their firewalls and intrusion detection system (IDS) detect a large amount of traffic coming from your IP to their product page, then they may conclude that your organization is planning to come out with a similar product.
- 2. IP-based blocking: This process is often used for blocking the access of specific IP addresses and/or domain names. For example, given the industrial espionage activities that are rampant these days, your marketing research team may be blocked from accessing your competitor's website, thus, limiting the marking team's ability to conduct industry and competitive intelligence for your firm.
- 3. IP-based "cloaking": Businesses are global in nature and economies are interconnected. There are websites that change their online content depending on a user's IP address or user's geographic loca-tion. For example, let us say your competitor web tool recognizes one of your technical employees surfing its site and displays incorrect or inaccurate product information to your IP address, thus, making it impossible to obtain accurate competitive information.

INTRODUCTION

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- 4. Cyberterrorism: "Cyberterrorism" refers to the direct intervention of a threat source toward your organization's website. One example of this occurred in year 1997, wherein the Pentagon simulated a cyberattack. Through this simulation, they found that attackers were using ordinary computers and widely available software that could disrupt military communications, electrical power and 9-1-1 networks in several cities in the US. Since then, hacking tools and expertise have become only more widespread.
- 5. Confidential information leakage: "Insider attacks" are the worst ones.Typically, an organization is protected from external threats by your firewall and antivirus solutions. However, an organization is not protected from the internal threats that occur everyday when employees surf the Internet and inadvertently give out confidential information over time. Your competitor can determine your strategic initiatives, such as a hostile takeover, based on the information that your employees pull from their

COST OF CYBERCRIMES AND IPR ISSUES

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Cyber crimes cost a lot to the organizations.
- When cyber crime incident 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.
- Trade secret or Intellectual Property (IP), when it leaves the organization, is considered as one of the biggest impacts of cybercrime.
- The benchmark study also showed that there are high costs associated with Malicious Code, viruses, web attacks and attacks by malicious insiders.
- It is the (a) "frequency of cybercrimes" along with (b) its success (i.e., cyber attacks that get through organization's firewalls and IDS) together that become a key reason for organizations to worry about the "cost of cybercrimes.“
- "Information theft" represents the highest external cost.

COST OF CYBERCRIMES AND IPR ISSUES

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

Internal Costs Associated with Cyber security Incidents

- The internal costs typically involve people costs, overhead costs and productivity losses.
- Benchmark study mentioned previously shows:
  1. Detection costs (25% - largest).
  2. Recovery costs (21%).
  3. Postresponse costs (19%).
  4. Investigation costs (14%).
  5. Costs of escalation and incident management (12%).
  6. Cost of containment (9% - lowest).
- “Attack vector" - this term is used to categorize an attack type.
- The cost of cybercrime varies depending on the attack type, industry type and organizational size. For example, the financial and defense sectors worldwide have attracted more cyberattacks than any other industry

COST OF CYBERCRIMES AND IPR ISSUES

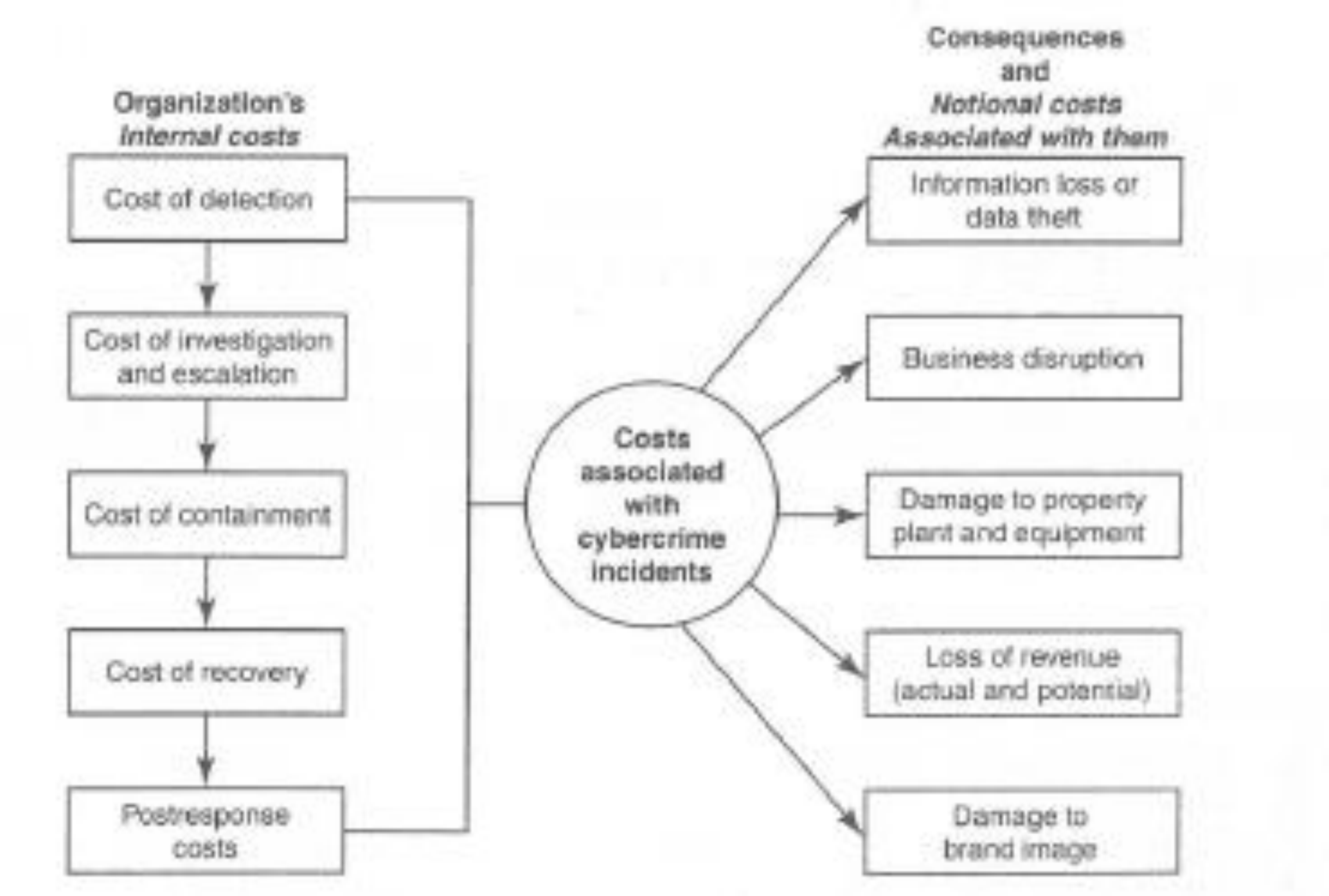

Organization's
Internal costs
Cost of detection
Cost of investigation and escalation
Cost of containment
Cost of recovery
Postresponse costs
Costs associated with cybercrime incidents
Consequences and
Notional costs Associated with them
Information loss or data theft
Business disruption
Damage to property plant and equipment
Loss of revenue (actual and potential)
Damage to brand image

Fig: Cost of Cyber Crimes

COST OF CYBERCRIMES AND IPR ISSUES

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- A CEO of an organization would like to focus on tools and automated methods to get better at detecting cybercrimes. Any tool that detects smartly would be on the CEO's shopping list!
- The consequences of cybercrimes and their associated costs, mentioned show a pattern (a benchmark study supported this:
  - 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 (1.3 %).
  - 5. Other costs (10%).
- There is a subjective element depending on the nature of an organization for example, revenue cos could be higher for a fully E-Commerce company that purely sells from the Web-based portal.

COST OF CYBERCRIMES AND IPR ISSUES

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- The percentage of organizations impacted by various types of cybercrimes show the following distribution:
  - Viruses, worms and Trojans (100%)
  - Malware (80%)
  - Botnets (73%)
  - Web-based attacks (53%)
  - Phishing and social engineering (47%)
  - Stolen devices (36%)
  - Malicious insiders (29%)
  - Malicious Code (27%)

- Average days taken to resolve cyber attacks are:
  - Attacks by malicious insiders (42 days - highest).
  - Malicious Code (39 days).
  - Web-based attacks (19 days).
  - Data loss due to stolen devices (10 days).
  - Phishing and social engineering attacks (9 days).
  - Viruses, worms and Trojans (2.5 days).
  - Malware (2 days).
  - Botnets (2 days).
- The many new endpoints in todays complex networks; they include hand held devices.

COST OF CYBERCRIMES AND IPR ISSUES

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Lessons to learn:
  1. Endpoint Protection
  2. Secure Coding
  3. HR Checks
  4. Access Controls
  5. Importance of Security Governance

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; violation of copyright laws (pirated software) makes company officials criminally liable under the Copyright); and "knowing use" is also a criminal offense under the Act. Use of unlicensed software, that is, pirated software, should be discouraged in the organization.
- One of the lapses exploited by cybercriminals is the vulnerability of nongenuine computer software. The spread of this virus can be partly attributed to the lack of automatic security updates for unlicensed software.

COST OF CYBERCRIMES AND IPR ISSUES

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Non-genuine software can potentially disrupt smooth functioning of an organization's operations by adversely affecting the system security infrastructure. 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.
- 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. It is possible to do this by establishing a software license tracker tool.
- Organizations that ignore the issue of pirated software could be exposing themselves to security risks, with implications such as loss of data, confidentiality, integrity, and reduced operational performance.
- Indirect threats of deploying non-genuine software include increased cost of protection, remediation and also a possibility of the organization/user becoming a part of a larger nexus of antisocial elements funding illegal software businesses and contributing to the network of organized crime

COST OF CYBERCRIMES AND IPR ISSUES

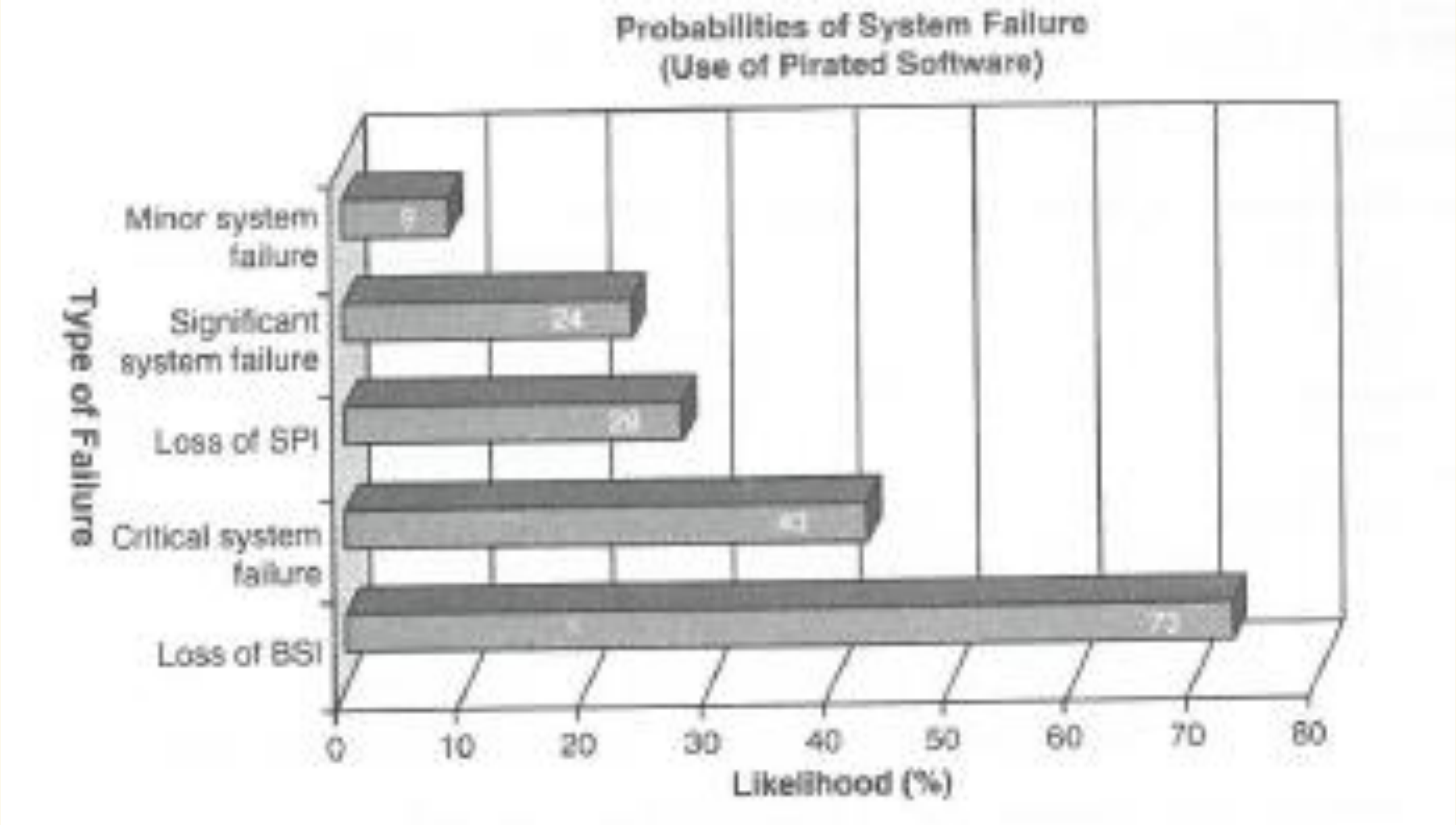


Fig: Probabilities of system failure (use of pirated software).

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- 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.
- There are web portals too in the E-Commerce model of doing business. Video and audio contents are delivered from the Web; software and infrastructure get delivered from the cloud! There is an inevitable dependence on the Internet. Therefore, cybercriminals find it convenient to use the Net for committing crimes.
- Employees expect to have Internet access at work just like they do at home.
- Mobility is picking up in India too though at a much limited pace compared to other countries. 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.
- Other concerns are about keeping Internet bandwidth available for legitimate business needs and ensuring uptime of applications and business websites.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- IT Managers should find a balance between allowing reasonable personal Internet use at work and maintaining office work productivity and work concentration in the office.
- From an organizational perspective, web threats can be classified into two broad categories.
  - First, employees do a number of activities online such as visiting infected websites, accessing pornographic sites, responding to Spam mails and attempting to hack sites (for legitimate and illegitimate reasons) to name a few.
  - Second, 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 handle an "incident" alert received.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- IT management is preoccupied with some of the top issues - they are described below:
- 1. Employees wasting time on social networking and similar sites (such as Facebook, Twitter, etc.) and its impact on employee productivity. With rise in workforce mobility, this is likely to affect even more as it is very difficult to monitor remote employee.
- 2. Enforcing "Acceptable Use Policies" is a challenge, especially, in very large, multi-location and3.matrix-structured organizations where getting the leaders to agree are a big challenge.
- 3. The difficulty in monitoring employees' web usage - there are tethered as well as remote employees; keeping them under watch constantly is next to impossible. Also, people are becoming increasingly aware about their "privacy rights.“
- 4. Keeping security systems up to date with patches and signatures is a challenge; this includes the challenge of operating system (OS) patches as well. We often hear about Microsoft vulnerability attacks. Most of us are busy installing one patch or the other on our laptops or desktops - it is theเก่ necessary evil in Windows world.
- 5. Legal and regulatory compliance risks (such as employees visiting inappropriate websites and the accidental disclosure of confidential information online). Laws are getting tough and regulatory compliance pressures are high especially in data breaches and employee privacy matters.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- 6. Keeping the Internet bandwidth free for legitimate business use - there are bandwidth-hungry applications such as live video conferencing, YouTube, online training modules, as class room-based faculty delivered face-to-face training is the thing of the past, etc.
- 7. Protecting remote workers and homeworkers (workforce mobility) - mobility of white collar workers is on the rise as mentioned.
- 8. Employees using unauthorized Web-based applications - this is indeed a challenge in a virtual team environment with employees spread across locations. Protecting the organization against Spyware and malware.
- 9. Remote filtering capabilities are incorporated into the newest versions of Websense. Web filtering and web security software restrict the use of Internet.
- 10. Protecting multiple offices and locations - these are effects of globalization and the emerging "follow-the-sun-model" wherein business never sleeps and customers' insistence on business continuity means that there are alternate locations acting as shadow sites.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Following are various types of mobile workers/remote workers:
- 1. Tethered/remote worker: This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems. This includes homeworkers, telecottagers, and in some cases, branch workers.
- 2. Roaming user: This is either an employee who works in an environment (e.g., warehousing, shop floor, etc.) or in multiple areas (e.g., meeting rooms).
- 3. Nomad: This category covers employees requiring solutions in hotel rooms and other semi-tethered environments where modem use is still prevalent, along with the increasing use of multiple wireless technologies and 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. This type includes the sales and field forces.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- There is another way, too, for classifying the workforce:
- 1. Office-based mobile workers: These are the ones who spend most of their time in a company-provided office, but they also sometimes work at home or in a third place.
- 2. Non-office-based mobile workers: These are the ones in the field, such as a salesperson, or workers between buildings on a corporate campus, such as IT professionals. They are more often at someone else's office than their own.
- 3. Home-based mobile workers: These are the former telecommuter; this employee class spends most of the week working in a home office, but comes into the corporate workplace for meetings or collaborative work sessions.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Organizations need not be hapless about handling these challenges to mitigate he associated risks for each of these challenges.
  1. Employee Time Wasted on Internet Surfing
  2. Enforcing Policy Usage in the Organization
  3. Monitoring and Controlling Employees’ Internet Surfing
  4. Keeping Security Patches and Virus Signatures Up to Date
  5. Surviving in the Era of Legal Risks
  6. Bandwidth Wastage Issues
  7. Mobile Workers Pose Security Challenges
  8. Challenges in Controlling Access to Web Applications
  9. The Bane of Malware
  10. The Need for Protecting Multiple Offices and Locations

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

1. 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.
- Organizations need to discipline an employee for Internet misuse. One way of doing that is through "Safe Computing Guidelines/Internet Usage Guidelines". However, these guidelines alone are not enough.
- Organizations need software tools, which, once installed, monitor employee Internet activities in the background. Cookies store the surfing activities.
- Employees wasting time online is a big issue for most organizations and at the same time the ways for complaining about it are getting limited.
- Take for example the developers; they have so many online groups and communities in the development network (e.g., the MSDN - Microsoft Development Network) that they need to refer. There are also blogs posted on the topic of bugs, numerous problems associated with software development, platform specific tips, etc.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Excessive web surfing consumes heavy bandwidth.
- Monitoring does keep IT department very busy dealing with disciplinary issues.
  - 1. Constantly monitor – classify the findings and report
  - 2. You need to hold meetings to discuss the issues-prepare action plan and report actions taken.
- Organizations need to take a permissible approach.

WEB THREATS FOR ORGANIZATIONS

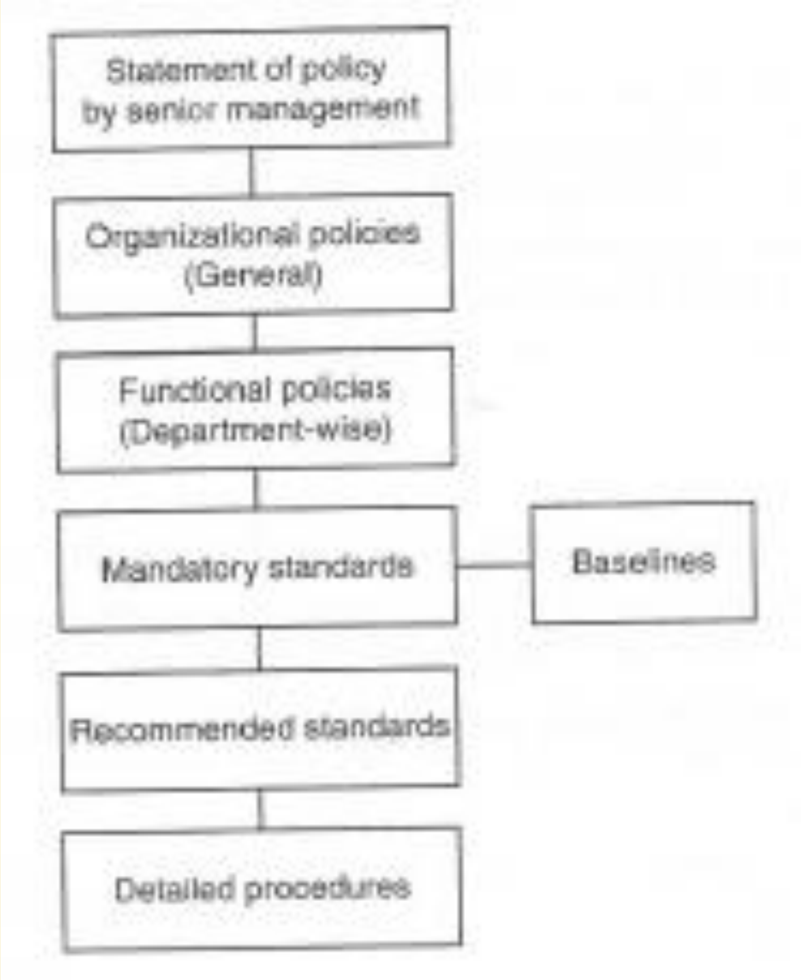
CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

2. Enforcing Policy Usage in the Organization

- An organization has various types of policies.
- A security policy is a statement produced by a senior management of a organization.
- Security policy is a codified set of processes and procedures applied to secure the fulfillment of its obligations and the continuation of its activities even in the presence of possible interferences.
- A security policy can be an organizational policy, an issue-specific policy or a system-specific policy. Most companies also have policies for acceptable use of the Internet.
- Its effective implementation draws from the continuous training to educate users about security policies.
- Inconsistent enforcement of policies and making security rules on the fly makes disciplinary action harder.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY



Statement of policy by senior management

Organizational policies (General)

Functional policies (Department-wise)

Mandatory standards

Baselines

Recommended standards

Detailed procedures

Fig: Policy hierarchy chart.

WEB THREATS FOR ORGANIZATIONS

- IPPs (Information Privacy Principles) set out general rules for organizations to apply:
  - 1. IPP1 - Collection: Manner and purpose of collection of PI.
  - 2. IPP2 - Use and disclosure: Solicitation of PI from individual concerned.
  - 3. IPP3 - Data quality: Solicitation of PI generally
  - 4. IPP4 - Data security: Storage and security of PI.
  - 5. IPP5 - Openness: Information relating to records kept by record-keeper.
  - 6. IPP6 - Access and correction: Access to records containing PI.
  - 7. IPP7 - Identifiers: Alteration of records containing PI.
  - 8. IPP8 - Anonymity: Record-keeper to check accuracy, etc., of PI before use.
  - 9. IPP9 - Transborder data flows: PI to be used only for relevant purposes.
  - 10. IPP10 - Sensitive information: Limits on use of PI.
  - 11. IPP11 - Limited disclosure: Limits on the disclosure of PI.
- Many cybercrimes take place by stealing people's PI.
- Privacy mature organizations understand this and they protect privacy of their employees, prospective employees, customers and prospective customers as well as associates

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

3. 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(ex: during lunch hours)
- Monitoring cookies give HR investigations and mangers a broad picture of company wide usage patterns.

4. Keeping Security Patches and Virus Signatures Up to Date

- Doing it properly and regularly absorbs a significant amount of time. At the same time, not doing it properly exposes IT systems to unnecessary risk. Typically 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.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

5. Surviving in the Era of Legal Risks

- most organizations get worried about employees visiting inappropriate or offensive websites.
- if employees download pirated software, then directors can personally be held liable.
- Similarly, downloading other inappropriate images result in a hostile environment for co-workers. Poorly judged or irresponsible comments made by employees on public Internet forums can be slanderous or breach of confidentiality guidelines.
- Organizations with effective web filtering and monitoring can provide reassurance and reduce risks.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

6. 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.
- At the same time, there is a considerable rise in workforce mobility and many remote connections to work networks are through the virtual private network (VPN).
- A considerable percentage of a business's bandwidth gets used for non-work Internet access. This indeed is a waste of money and it reduces the bandwidth available for legitimate work. The result is slower E-Mail, slower web browsing and slower VPN connections.
- There are tools to protect organization's bandwidth by stopping unwanted traffic before it even reaches your Internet connection. Using sophisticated policy controls, you can get such tools to block banned websites, downloads, E-Mail Spam and media streams your own systems before they reach your network.
- This helps increase work productivity by preserving the bandwidth for real work.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

7. Mobile Workers Pose Security Challenges

- Most mobile communication devices - for example, the personal digital assistant (PDAs) and RIM BlackBerries - have raised security concerns associated with their use.
- Mobile workers use those devices to connect with their company networks when they are on the move. Even if organizations have in-house systems to monitor and control web access and to protect web users from malware, those systems often may not be capable of covering remote users working on laptops and homeworkers operating outside the corporate firewall. This means that there is a significant part of the workforce that remains unprotected. Most organizations see this as a serious issue that can threaten organizational security.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

8. 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; now cloud computing too is added to that repertoire.
- For example, an employee was unable to use his/her company mail application or perhaps was unable to access the mail server of the company when sending information that was urgent in business context. Instances such as these reduce IT department's control over data and security. More and more organizations are getting worried about employee access to webmail or instant messaging applications.
- You can select tools that provide granular control over which sites are allowed and which are banned from being accessed. It is possible to limit access to personal sites during office hours with time limits.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

9. The Bane of Malware

- 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 consequences of infection are severe compared with any kind of malware.
- It saps organization's energy because virus clean-up takes time, diverts IT resources and costs money. Infection makes company's confidential information vulnerable and undermines the IT department's efforts to provide assurance to the board about security.
- Due to this, it becomes essential to have protection that goes beyond signature detection. There are tools and services that offer a combination of signature scanning and advanced heuristic protection using proprietary technology. It looks like producing malware and Malicious Codes have become an industry within the organized criminal syndicates.

WEB THREATS FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -

10. The Need for Protecting Multiple Offices and Locations

- 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, you need anti-malware, web filtering and monitoring software and all the support needed to keep it up to date.
- Additional effort is required with multiple sites, as all hardware and administrative overheads are multiplied! In such a scenario, an Internet-based-hosted service that can easily protect many offices is worth considering.
- 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.
- Fixed fee per user is also an option to consider.

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

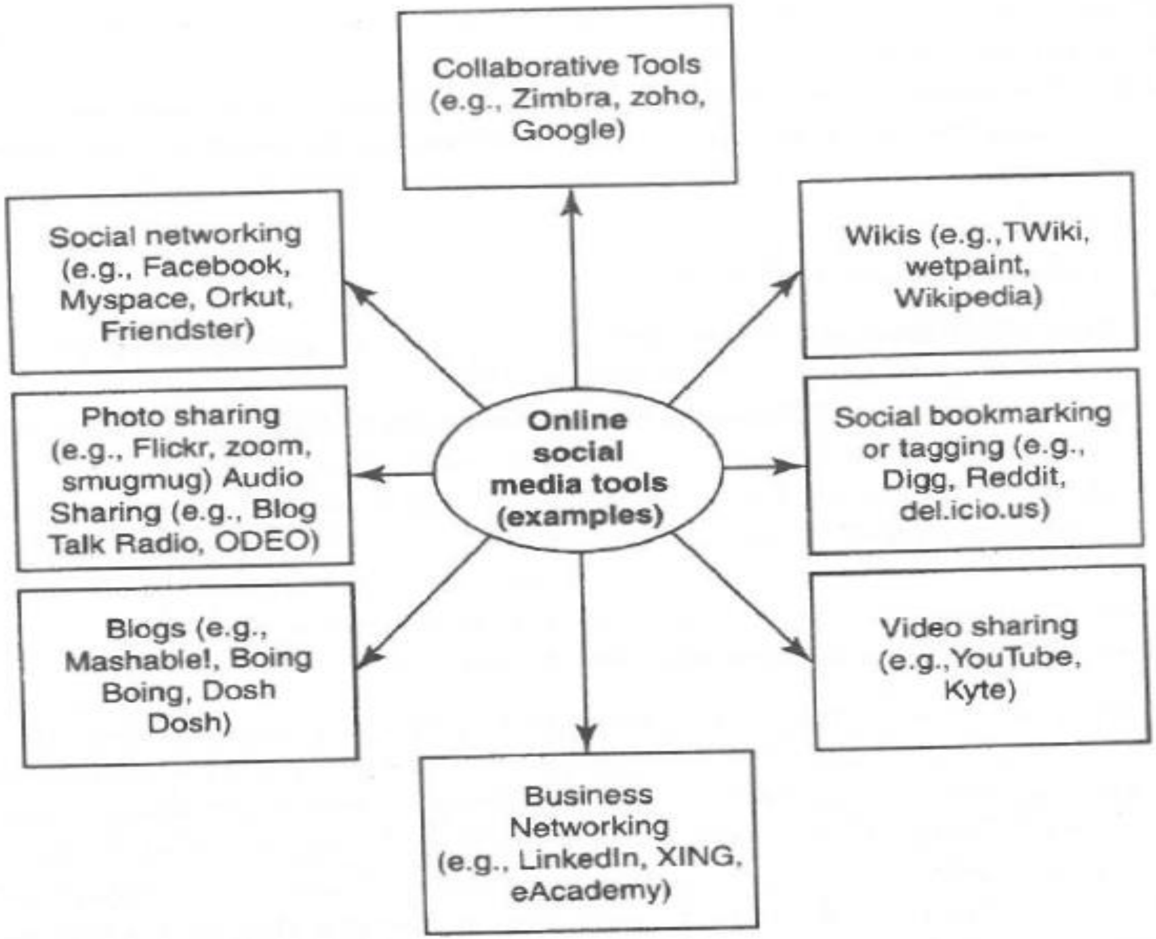
- Of late, social media marketing has become dominant in the industry.
- Survey by marketing professionals, usage of social media sites by large business-to-business (B2B) organizations shows the following: 1. Facebook is used by 37% of the organizations.2. LinkedIn is used by 36% of the organizations.1ว่Twitter 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.
- The Internet has penetrated India in a big way and due to this security breach incidences are on the rise. Hackers use a number of Internet channels such as the Web, E-Mail, instant messaging, Voice over Internet Protocol (VoIP), etc. to launch sophisticated and targeted attack to steal information from which they can benefit financially.

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Although the euphoria about social media marketing practice is high (seems mainly due to competitive pressures), organizations must protect their data.
- 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.“
- “Social media marketing" is an approach that makes use of social media sites to enhance the visibility on the Internet so as to promote products and services. People find that social media sites are useful for building social (and business) networks and for exchanging ideas and knowledge.

SOCIAL MEDIA MARKETING


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)
Online social media tools (examples)
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)

Social Media- Online Tools

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY -

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, etc.
- Following are the most typical reasons why organizations use social media marketing to promote their products and services:
  - To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertising fees.
  - 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.
  - To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertising campaign.

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

  - To build credibility by participating in relevant product promotion forums and responding to potential customers‘ questions immediately.
  - To collect potential customer profiles. Social media sites have information such as user profile data, which can be used to target a specific set of users for advertising.
- In addition to the social media online tools mentioned in, 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 community of 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.

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

Best Practices with Use of Social Media Marketing Tools

- First and foremost, it is essential to establish a "social media policy." Use of personal blogging for work-related matters should be monitored and minimized.
- "Employee Time Wasted on Internet Surfing" about employees endlessly surfing on the Internet during the work hours.
- "Enforcing Policy Usage in the Organization". Once the policy is created, employers should communicate it to employees and should enforce its implementation through continuous monitoring.
- Increasing employee awareness is an ongoing activity. There is no go without it. This is because people can change their way of behaving in social networks only if they are aware of the security risks; sometimes they are genuinely not aware of those risks.

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- There is a strong need to establish firm processes that are systematically linked to daily workflows. Such processes should be easy to implement and audit. For example, administrators should ensure that the latest security updates are downloaded. Although it seems to be mundane and boring activity, it is crucial.
- Organizations must enable their IT administrators to identify network attacks in time or to avoid them altogether. IDS and firewalls play a crucial role here.
- “Need-based access policy", with this it becomes possible to control and monitor access to critical data, and to track such access at any time. Doing this reduces the risk of information falling into wrong hands through unauthorized channels.

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Blocking the infected websites is another necessary activity.
- Access blocking can also be applied to any other suspicious site on the Internet. The filter function should be kept continuously up to date by maintaining so-called black- and white-listed websites.
- Using next-generation firewalls helps organizations keep their security technology up to date. Some firewalls provide a comprehensive analysis of all data traffic. Deep inspection of network traffic makes it possible to monitor the type of data traffic, the websites from which it is coming, to know the web browsing patterns and peer-to-peer applications to encrypted data traffic in SSL tunnel.
- Protection against vulnerability is possible by carefully planning vulnerability scanning and penetration testing. An intrusion prevention system (IPS) serves as a protective barrier to the corporate network.

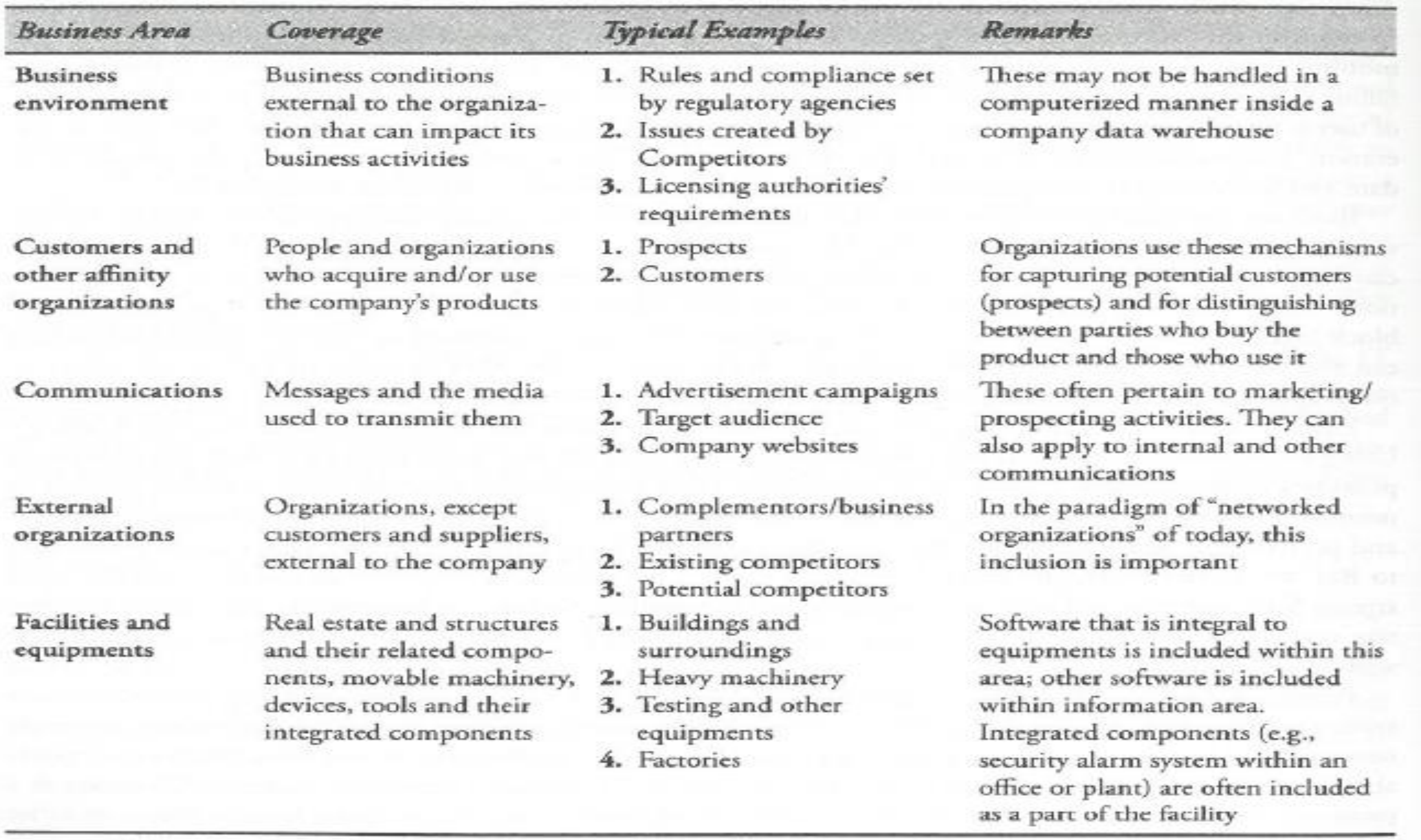
SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Having identified an attack, the IPS immediately stops it and prevents it from spreading in the network. The IPS also enables patching of servers and services by securing servers under security threat, which will then be patched during the next maintenance window.
- Within this group, the use of social media can be monitored only on a very limited basis or not at all. This makes it even more important to assign the rights for defining all network access centrally, for example, using an SSL VPN portal - VPN is virtual private network, a tunnel within the Internet.
- The user level a strong authentication via single sign-on makes the administrator's work easier.
- Even the Intranets are not spared by cyber attackers. Therefore, securing the Intranets should also be included in the protector activities. The Intranet of every company contains highly sensitive information pertaining to the business areas involved.

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY



Business Area	*Coverage*	*Typical Examples*	*Remarks*
Business environment	Business conditions external to the organization that can impact its business activities	1. Rules and compliance set by regulatory agencies 2. Issues created by Competitors 3. Licensing authorities' requirements	These may not be handled in a computerized manner inside a company data warehouse
Customers and other affinity organizations	People and organizations who acquire and/or use the company's products	1. Prospects 2. Customers	Organizations use these mechanisms for capturing potential customers (prospects) and for distinguishing between parties who buy the product and those who use it
Communications	Messages and the media used to transmit them	1. Advertisement campaigns 2. Target audience 3. Company websites	These often pertain to marketing/prospecting activities. They can also apply to internal and other communications
External organizations	Organizations, except customers and suppliers, external to the company	1. Complementors/business partners 2. Existing competitors 3. Potential competitors	In the paradigm of "networked organizations" of today, this inclusion is important
Facilities and equipments	Real estate and structures and their related components, movable machinery, devices, tools and their integrated components	1. Buildings and surroundings 2. Heavy machinery 3. Testing and other equipments 4. Factories	Software that is integral to equipments is included within this area; other software is included within information area. Integrated components (e.g., security alarm system within an office or plant) are often included as a part of the facility

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

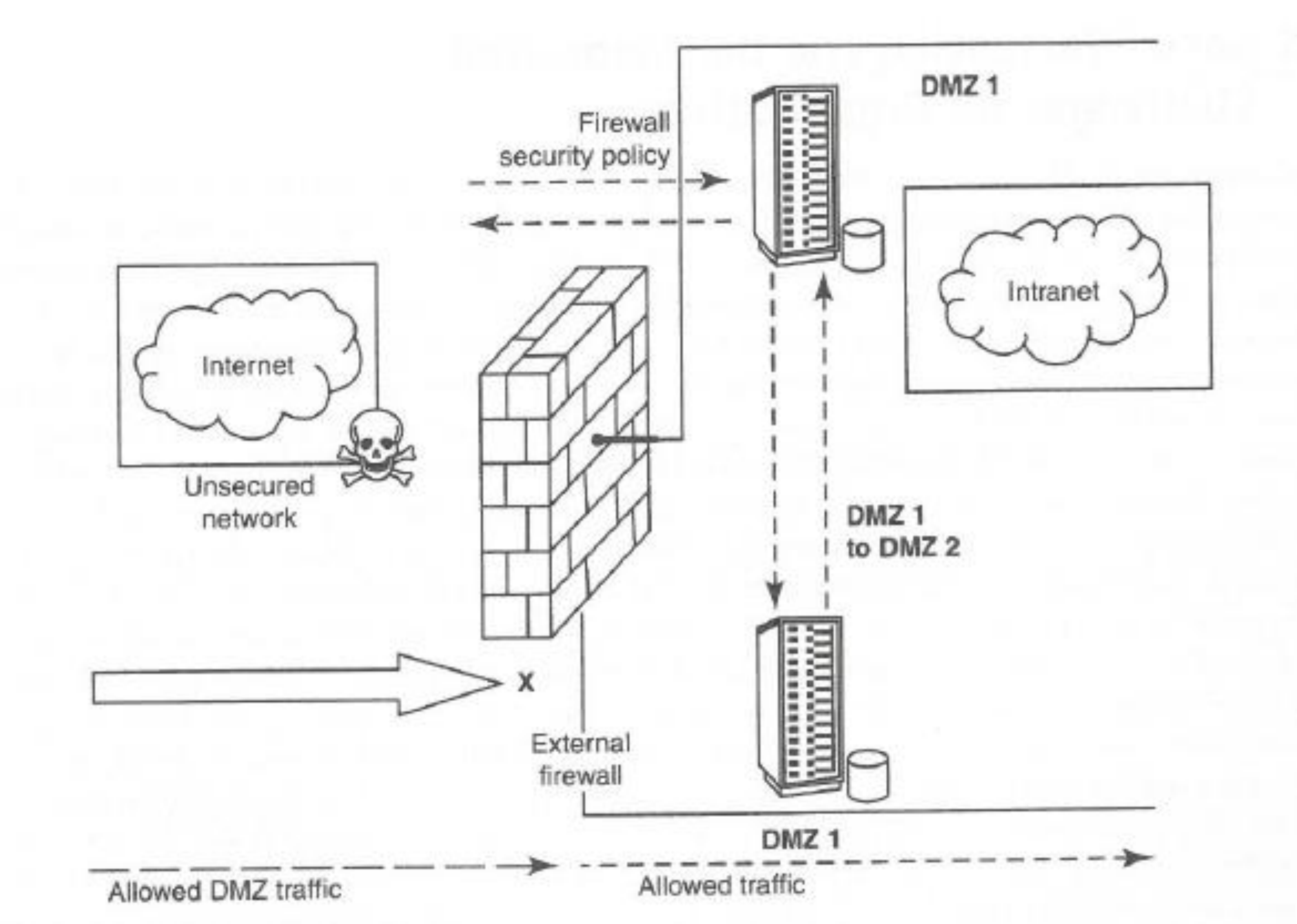
- These areas need to be isolated from the rest of the internal network by using the firewalls to segment the Intranet. This enables segregation of departmental Intranets; for example, a company can separate departments such as finance or accounting from the rest of the Intranet and thereby prevent infections from penetrating these critical segments of the corporate network.
- If there is a need to use an existing multiple network segments then you can deploy multiple DMZ with differing security policies (levels). For example, you may need to deploy the applications for Extranets, Intranets, web server hosting and remote access gateways

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- The corporate security department, therefore, needs to include mobile devices in the security policies. This can be done, for example, with the assessment function by checking the login device for the required security settings and for the presence of security-relevant software packages.
- Through this function, it can be checked whether the proper and latest host firewall is installed and whether both the OS and antivirus software as well as all patches are up to date.

SOCIAL MEDIA MARKETING



Firewall with DMZ networks

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- On the basis of necessity warranted by a situation, mobile devices can be forwarded directly to a website containing the required updates.
- With the use of centralized management, administrators can manage, monitor and configure the entire network and all devices using a single management console. They can also monitor user activities on the network by viewing reports. For example, system administers will be able to know who has accessed which data at what time. This allows preventing attacks more effectively and provides more efficient protection for corporate applications at risk.
- A central management console also makes it possible to roll out and maintain standard security guidelines for the entire corporate network.

SOCIAL MEDIA MARKETING

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Given these issues, risks and challenges involved with the use of social media marketing tools, indeed the involvement of the senior employees of the organization is critical to the success of the social media marketing initiative.
- The organizational best practices are listed below:
  - 1. Organization-wide information systems security policy;
  - 2. configuration/change control and management;
  - 3. risk assessment and management;
  - 4. standardized software configurations that satisfy the information systems security policy;
  - 5. security awareness and training;
  - 6. contingency planning, continuity of operations and disaster recovery planning;
  - 7. certification and accreditation

SOCIAL COMPUTING AND THE ASSOCIATED CHALLENGES FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Social computing is also known as "Web 2.0" - it empowers people to use Web-based public products and services. Social computing 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.
- In the modern era, we are "constantly connected," business is "24 x7" - the business where world never sleeps. People carry anxieties in a competitive business world. In such a milieu, people and organizations are appreciating the "power of social media." Business is taken forward based on how connections are made through social networks.
- In this process, a lot of information gets exchanged and some of that could be confidential, Personally Identifiable Information (PII)/SPI, etc.

SOCIAL COMPUTING AND THE ASSOCIATED CHALLENGES FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- There is a new genre of challenges, though they come with rising use of social computing and organizations need to watch for these challenges. For example, social computing poses the risk of "digital divide." Getting too used to readily available information, people may get into the mode of not questioning the accuracy and reliability of information that they readily get on the Internet.
- With social computing, there are new threats emerging; those threats relate to security, safety and privacy.
- How to protect one's online privacy is in fact a major preoccupation for people all over the world; particularly in European countries where there is a very high consciousness about privacy loss.

SOCIAL COMPUTING AND THE ASSOCIATED CHALLENGES FOR ORGANIZATIONS

CYBER SECURITY - CYBER SECURITY - CYBER SECURITY - CYBER SECURITY

- Impersonation and identity, Cyber bullying and online grooming are new emerging threats.
- Data ownership and lack of controls in users hand for guarding their data are resulting in privacy invasion.
- Care should be taken while using social media when communicating with internal or external stake holders.