UNIT V
Cyber Security Organizational Policies, Risk and Challenges

Cybersecurity: Organizational Implications

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.

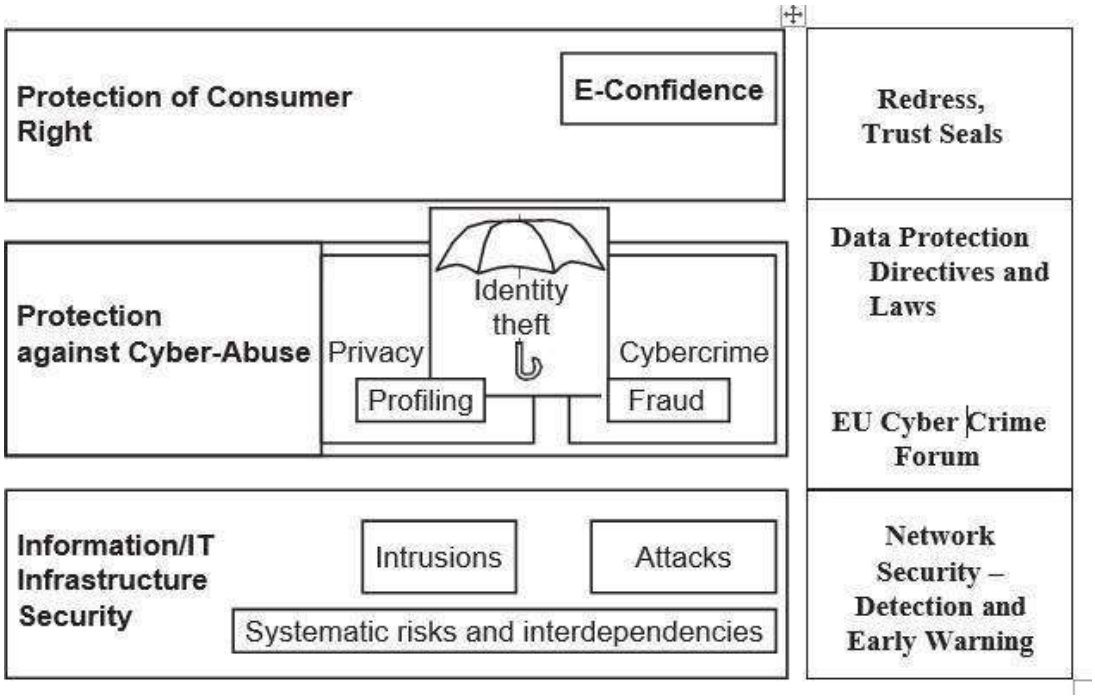


Fig: A cybersecurity perspective. EU is the European Union.

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 andother ‘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/oravailability.
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.

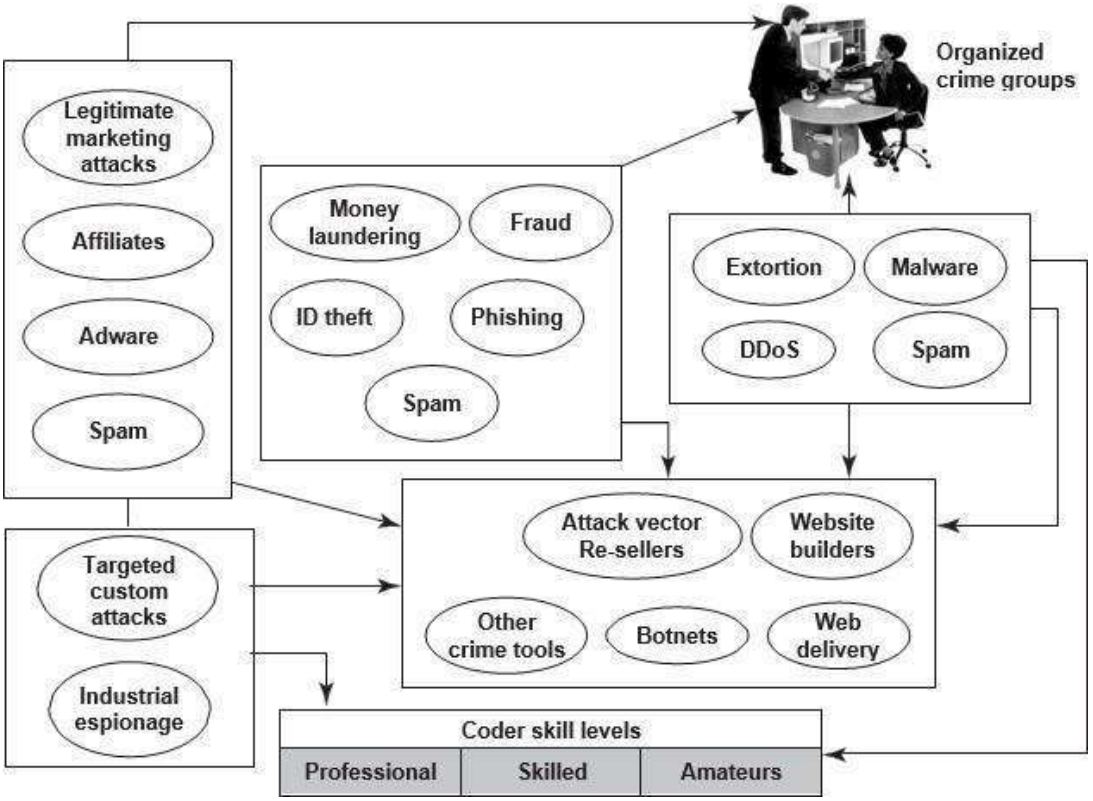


Fig: Cybercrimes – the flow and connections.

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.

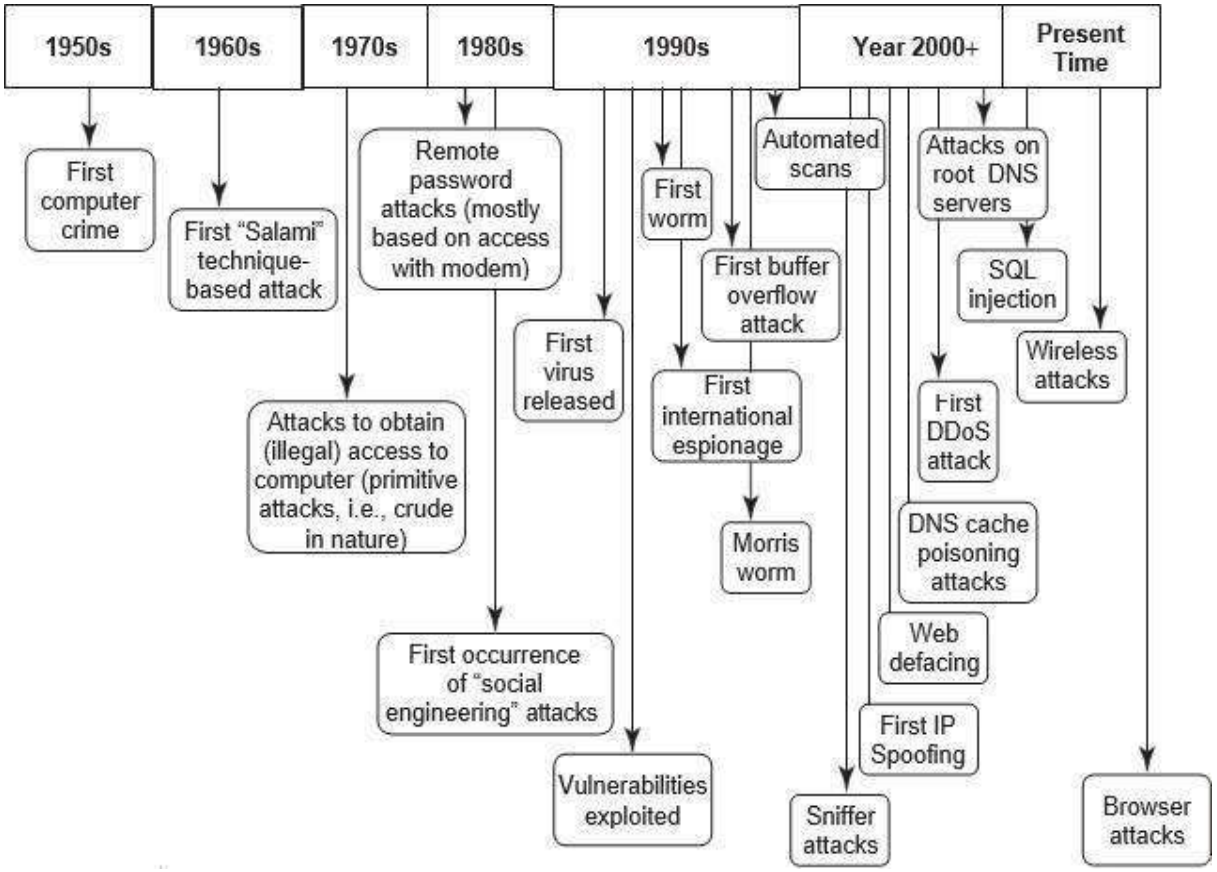


Fig: Security threats – paradigm shift.

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

➔ **Cost of Cybercrimes and IPR Issues: Lessons for Organizations**

Reflecting on the discussion in the previous sections brings us to the point that cybercrimes cost a lot to organizations.

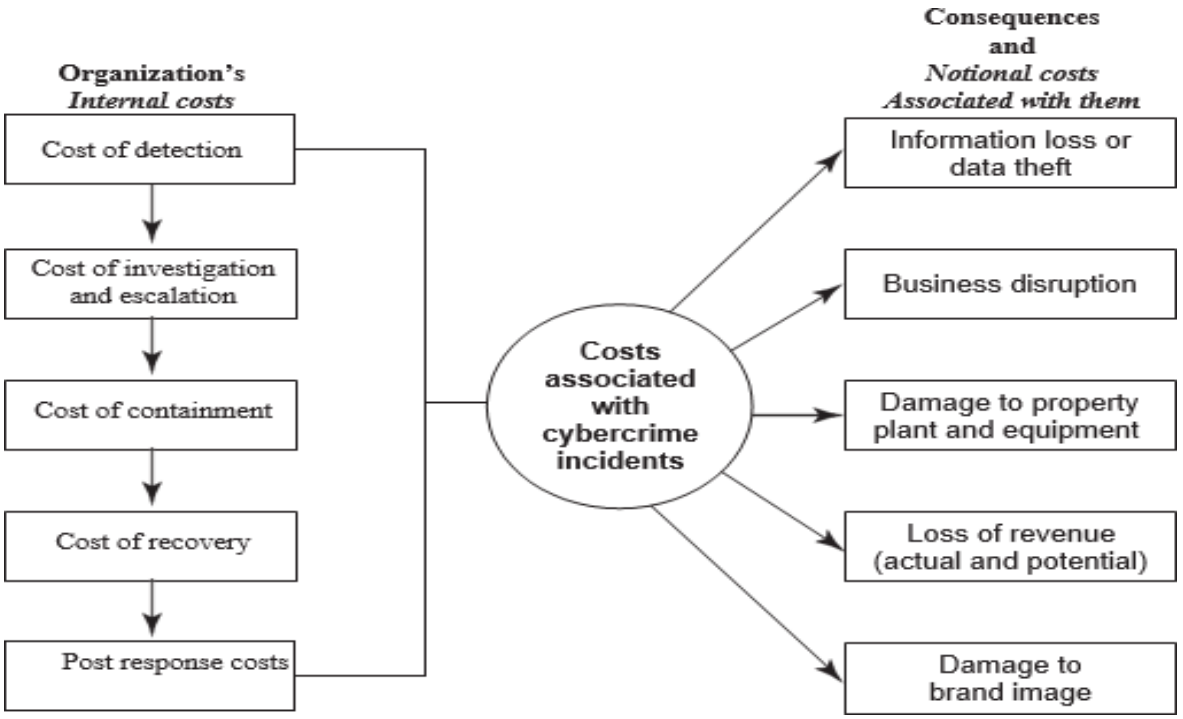


Fig: Cost of cybercrimes.

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 Cybersecurity 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.
2. Recovery costs.
3. Post response costs.
4. Investigation costs.
5. Costs of escalation and incident management.
6. Cost of containment.

- **The consequences of cybercrimes and their associated costs, mentioned**
  1. Information loss/data theft.
  2. Business disruption.

3. Damages to equipment, plant and property.
4. Loss of revenue and brand tarnishing.
5. Other costs.

- **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.

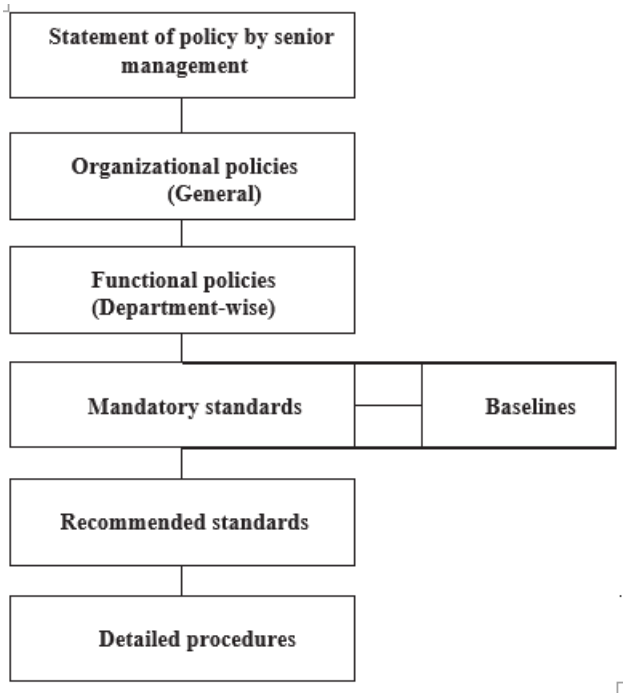


Fig: Policy hierarchy chart.

- **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 assistant

- **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.

- **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.

➔ **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:

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."

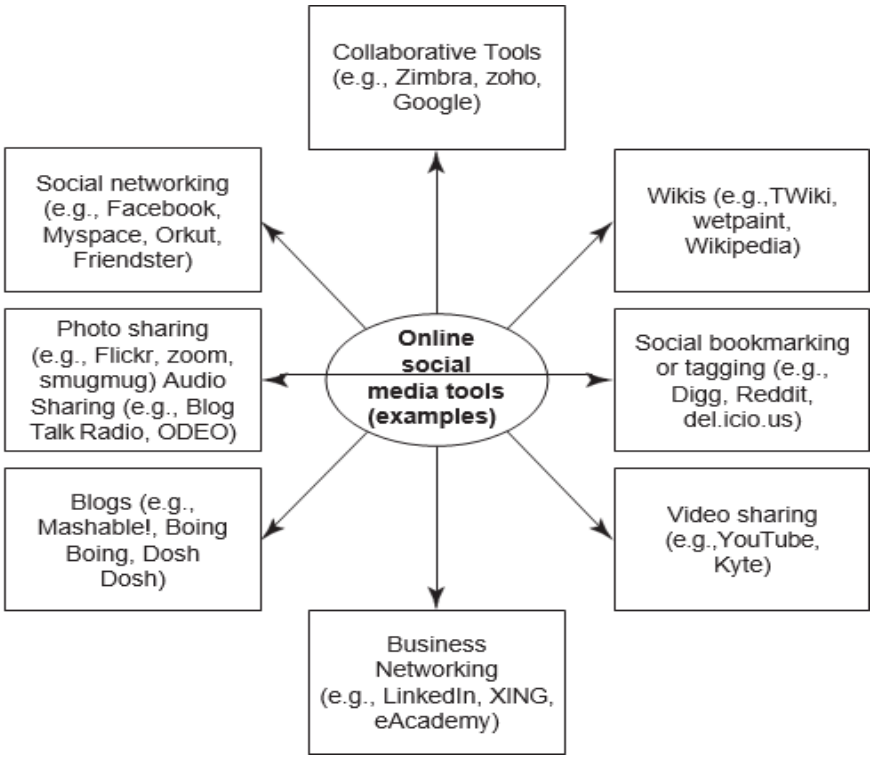


Fig: Social media - online tools.

- **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.

WHAT IS SOCIAL COMPUTING?

The social and interactive aspect of online activity is known as social computing. The phrase may be interpreted in contrast to personal computing, which refers to the activities of single users.

Blogs, wikis, Twitter, RSS, instant messaging, multi-gaming, and open source development are just a few examples of social computing. It also includes social networking and social bookmarking sites. The concept of Web 2.0 can be interpreted as the architecture for applications that support its processes. The term "social computing" is somewhat of a misnomer. It should not be implied that social computer applications are the same as artificial intelligence programs such as socially intelligent computing. The computer is required to exhibit social capabilities and make the person using it feel more socially engaged when they are not.

BENEFITS OF SOCIAL COMPUTING

Social networking allows organizations to do many things, including disseminating information among its various users, keeping them up to date on new knowledge and experience, reducing interruptions, and connecting them with the best experts for particular needs.

The notion of "social computing" refers to increasing knowledge access speed. In addition, it allows for a wide range of information to be shared through interactions with numerous people. By connecting people and thus lowering the cost of communication, computer technology improves communication among many users. The methodology improves user performance and efficiency, increasing access to specialists. Users obtain a better performance and greater efficiency due to this method.

Social computing reduces traveling expenses since it is linked to the internet process, lowering labor and travel costs. As employee satisfaction rises, so does its role in improving performance and quality of service.

EXAMPLES OF SOCIAL COMPUTING

Social computing uses computers and software to create communities around shared interests. All of these examples and blogs, wikis, Twitter, RSS, instant messaging, multiplayer gaming, open-source development, and social networking and social bookmarking sites are all forms. Web 2.0 is closely linked to the notion of social computing.

Many less obvious kinds of social computing are accessible to us today. Consider eBay, where buyers can leave user reviews of sellers and their responses. Look to Amazon, where you may now rate the reviewer rather than only the product.

Security and Privacy Implications from Cloud Computing

There are data privacy risks associated with cloud computing. Basically, putting data in the cloud may impact privacy rights, obligations and status. There is much legal uncertainty about privacy rights in the cloud. Organizations should think about the privacy scenarios in terms of "user spheres."

There are three kinds of spheres and their characteristics are as follows:

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.
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.

➔ **Protecting People's Privacy in the Organization**

The costs associated with cybercrimes. A key point in that discussion is that people perceive their PI/SPI to be very sensitive. From privacy perspective, people would hate to be monitored in terms of what they are doing, where they are moving.

In the US, Social Security Number is a well-established system/mechanism for uniquely identifying all American citizens; however, similar thoughts are now emerging in India. The UID Project was started by Government of India and is running through an agency called Unique Identification Authority of India (UIDAI) based on the similar concept.

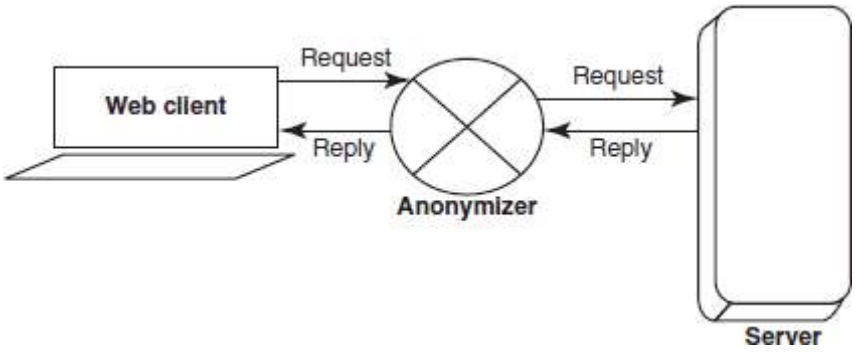
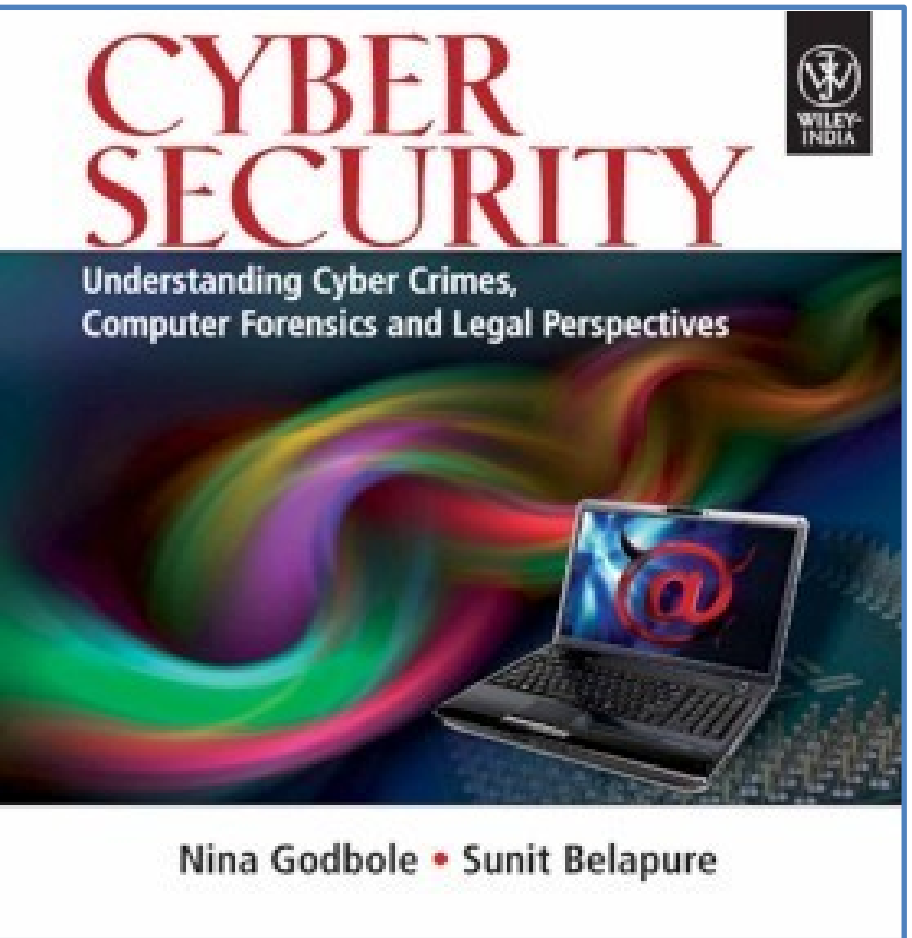


Fig: Anonymity by web proxy.

Chapter 9
Cybersecurity: Organizational Implications



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. 1).

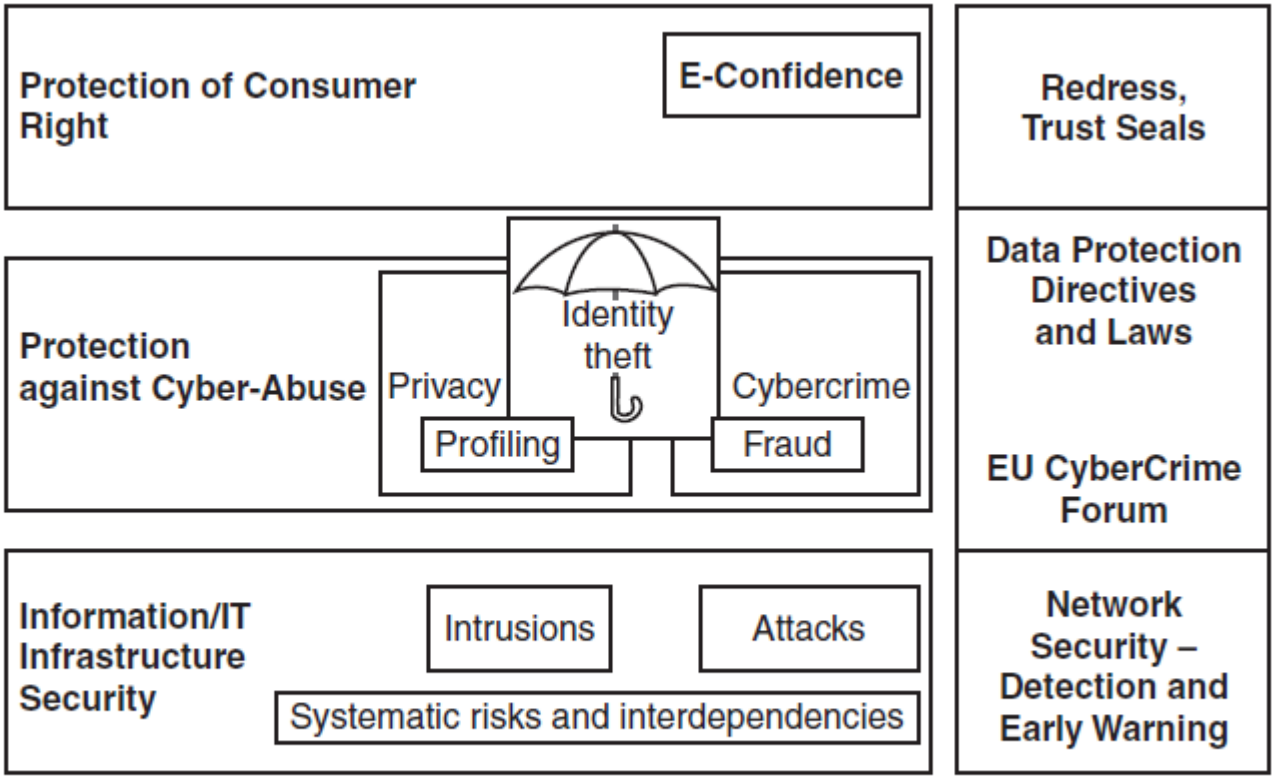


Figure 1 | A cybersecurity perspective. EU is the European Union.

Security breach

- Unauthorized acquisition of data that compromises security, confidentiality or integrity of personal information (PI).
- Good faith acquisition of PI either by an employee or an agent of an organization for business purposes is not considered to be a breach, provided that the PI is not used or subjected to further unauthorized disclosure.
- 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.

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 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.

Four key dimensions of Privacy:

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

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

The internal costs typically involve people costs, overhead costs and productivity losses (Fig. 2):

Internal costs associated with a cybercrime incidence

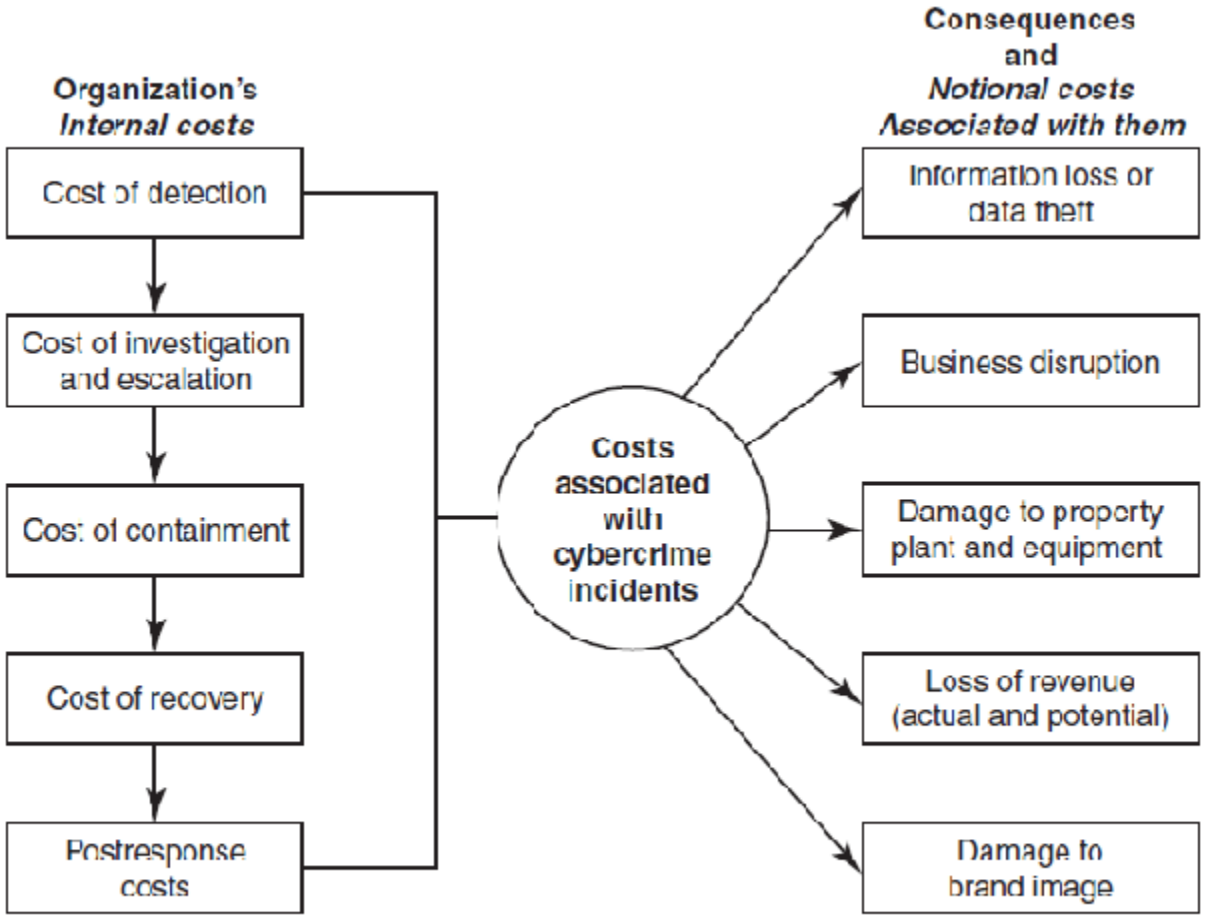


Figure 2 | Cost of cybercrimes.

The 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 (see Fig. 3). The spread of this virus can be partly attributed to the lack of automatic security updates for unlicensed software.

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.

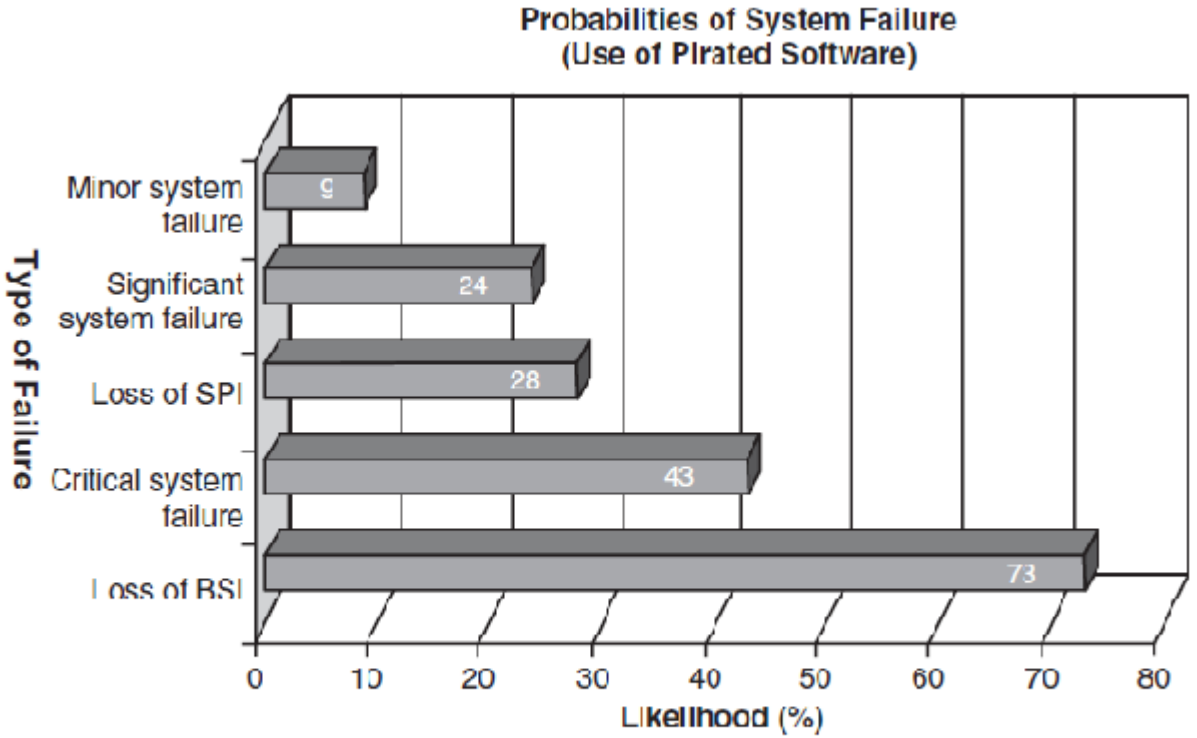


Figure 3 | Probabilities of system failure (use of pirated software).
SPI is sensitive personal data and BSI is business sensitive information.

Overview of 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, accessing pornographic sites, 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 handle an "incident" alert received.

Employee Time Wasted on Internet Surfing

3. Approximately 45–60 minutes spent on personal web surfing at work.
4. Safe Computing Guidelines/Internet Usage Guidelines should be implemented.
5. Organizations need software tools to track.

Keeping Security Patches and Virus Signatures Up to Date

- ✓ Updating security patches and virus signatures have now become a reality of life and 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.
- ✓ 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.

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 organization's bandwidth by stopping unwanted traffic before it even reaches your Internet connection.

Mobile Workers Pose Security Challenges

- Security concerns with Personal digital assistant (PDAs).
- Association of RIM BlackBerries.
- Mobile workers use those devices to connect with their company networks when they are on the move.

Challenges in Controlling Access to Web Applications

- Presently, 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.
- Employees often tend to use these applications to bypass corporate guidelines on security. Employees may use their personal E-Mail IDs to send business-sensitive information (BSI) for valid or otherwise reasons. 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.
- As the sophistication of online applications increases, this is going to become a significant problem.

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, cyberattackers, too, are learning. Criminals change their techniques rapidly to avoid detection. The consequences of infection are severe compared with any kind of malware.

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.
- 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 inhouse 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.

Security and Privacy Implications from Cloud Computing

There are data privacy risks associated with cloud computing.
Basically, putting data in the cloud may impact privacy rights, obligations and status.
There is much legal uncertainty about privacy rights in the cloud.
Organizations should think about the privacy scenarios in terms of “user spheres.”

Social Media Marketing: Security Risks and Perils for Organizations

Usage of social media sites by large business-to-business (B2B) organizations (Fig. 4):

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

Most typical reasons why social media marketing is used to promote their products and services:

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.

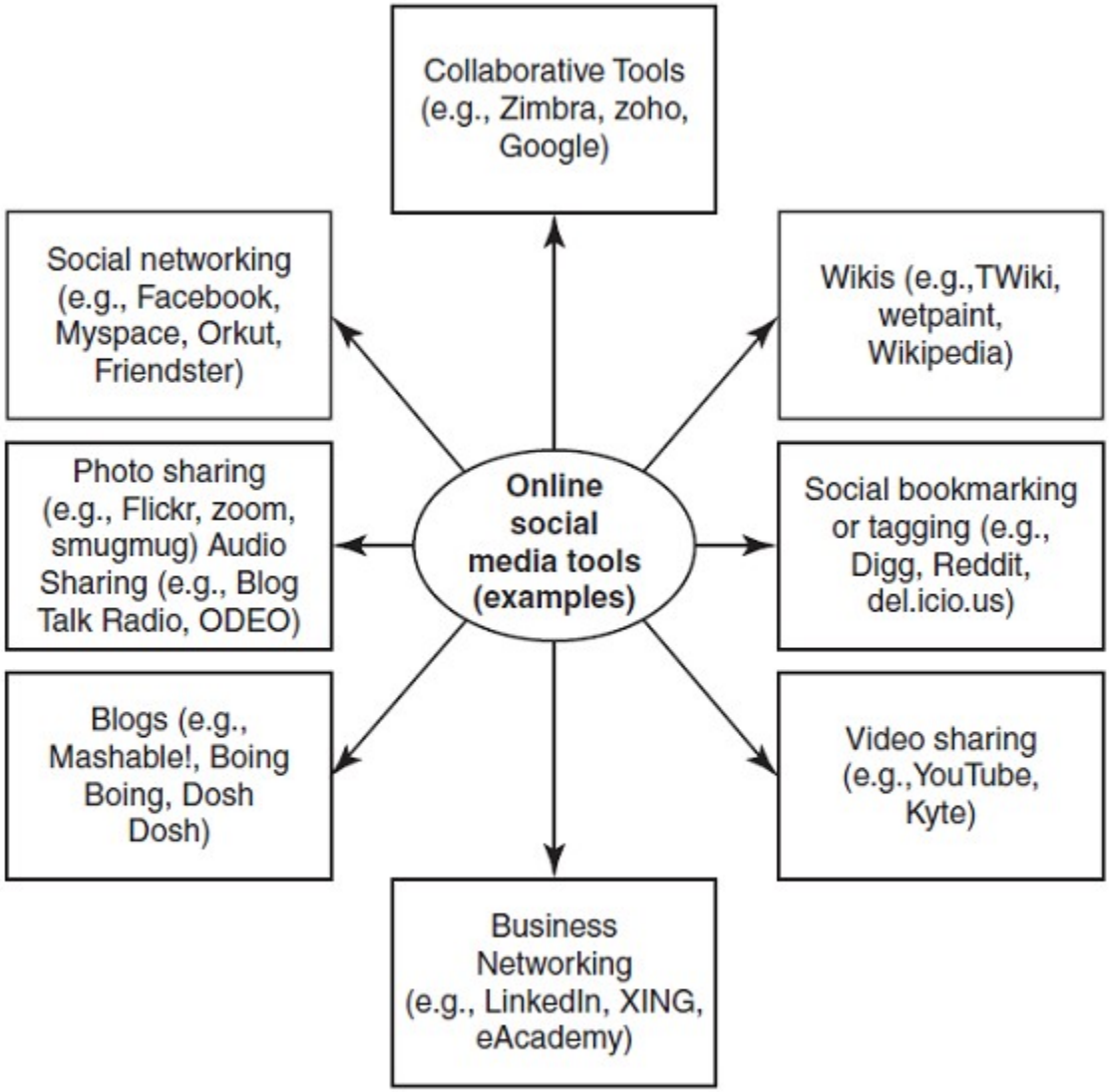


Figure 4 | Social media – online tools.

Best Practices with 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 appointment of a social media expert within the company.
- ✓ Need to establish the "need-based access policy."
- ✓ Policies should not be treated as a one-time activity.
- ✓ Blocking the infected websites is another necessary activity.
- ✓ Access blocking can also be applied to any other suspicious site on the Internet.
- ✓ Firewalls help to protect the organization.
- ✓ 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.
- ✓ Securing the Intranets should also be included in the protection activities.
- ✓ Include mobile devices in the security policy.
- ✓ With the use of centralized management, administrators can manage, monitor and configure the entire network and all devices using a single management console.

The Organizational Best Practices

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

1. Social computing (or "Web 2.0"): Empowers people to use Web-based public products and services.
2. It is much more than just individual networking and entertainment.
3. 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.
4. Social networking, social media marketing and social computing are not unrelated concepts.
5. Social computing is related to social media marketing.
6. Due care to be taken while using social computing as a channel strategy for communicating with internal or external stakeholders.

Protecting People's Privacy in the Organization

- ✓ People hate to be monitored
- ✓ Tracking and monitoring people's transactions on the Internet is a controversial issue.
- ✓ RFIDs have been successful to track objects, animals, birds and goods in shipment.
- ✓ In the US, Social Security Number is a well-established system/mechanism for uniquely identifying all American citizens.
- ✓ Although the Indian Government has issued IDs, they are fragmented by purpose and region in India.
- ✓ This leads to widespread bribery, denial of public services and loss of income – it particularly makes citizens poor.
- ✓ 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 existing in India are supposed to be linked to it.

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

Recognize the need for proactively protecting company's identity when online. Anonymizer effectively mitigates threats with their identity protection and information assurance solutions; however, there are risks too associated with "Anonymizers". In view of the cyberthreats, it becomes cardinally important for organizations to develop Safe Computing Guideline. They are sometimes referred to as Organizational Guidelines for the Internet Usage or Computer Usage Policy. Policies are always important as they provide an objective and direction for implementation.

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 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).

Cyber Security

- ➢ Protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

- Providing security in terms of both physical security to the devices and security to the information stored therein such devices.
- Providing protection from unauthorized access, use, disclosure, disruption, modification and destruction to both physical device and the information stored therein.

"Incident response," "incident handling" and "incident management" have a relationship among them. Incidents include but are not limited to the following list:

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 mis-configuration

"Event" and "adverse events" are the two related terms to be noted. An event is an observable occurrence in a system or network. All events may not call for a countermeasure unless they are "adverse events" which sometimes are referred to as "risk events." Adverse events are events that result in negative consequence.

On-call procedures are activated and vendor support is invoked:
1.High priority incidents
2.Medium priority incidents
3.Low priority incidents

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.

What Organizations Can Do To Protect their Systems from Cyber Security Incidents?

- ✓ Organizations need to protect their information systems from malware.
- ✓ Organizations need to protect business-sensitive information in general and protected health information (PHI) in the healthcare sector, and PI and SPI of their multiple stakeholders.

Best Practices for Organizations

1.Develop and implement an approach to malware incident prevention.
2.Develop and implement policies that support the prevention of malware incidents.
3.Incorporate prevention of malware incident and handling of awareness programs, and provide guidance and training to users.
4.Establish capabilities to mitigate vulnerabilities and to help prevent malware incidents through documented policy, technical processes and procedures.
5.Establish threat mitigation capabilities to assist in containing malware incidents by detecting and stopping malware before it can affect systems.
6.Establish a robust incident response process capability that addresses malware incident handling through preparation, detection and analysis, containment/eradication/recovery and post-incident activities.
7.Establish malware incident prevention and handling capabilities that address current and short-term future threats that are robust and flexible.

Incident Response Team Work, Capabilities and Structure

- ✓ An active coordination and management role needs to be created.
- ✓ 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.

Benefits from 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.
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.

Forensics Best Practices for Organizations

- Organization's forensics readiness is important.
- Forensics readiness is defined as the ability of an organization to maximize its potential to use digital evidence while minimizing the costs of an investigation.
- Preparation to use digital evidence is not easy.
- It involves system and staff monitoring, technical, physical and procedural means to secure data to evidential standards of admissibility, processes and procedures.
- All this becomes essential for ensuring that staff recognizes the importance and legal sensitivities of evidence, and appropriate legal advice and interfacing with law enforcement.
- The prime factor in understanding the need for forensics readiness is a risk assessment.
- An asset register is certainly needed to understand the attractiveness of targets to the types of crime
- Be aware that any information security defensive measures based on a risk assessment will always leave a residual risk.

Digital Forensics Investigation and Digital Evidences

- Quality and availability of evidence is a passive aspect of the DFI.
- Cybercriminals are known to exploit the fact that investigation is costly and takes time.
- Real-life situations show that half an hour of attacker time requires an average investigation time of 48 hours!

Digital evidence could:

- ✓ Help manage the impact of some important business risks.
- ✓ Support a legal defense.
- ✓ Support a claim to IPR.
- ✓ Show that due care (or due diligence) was taken in a particular process.
- ✓ Verify the terms of a commercial transaction.
- ✓ Lend support to internal disciplinary actions.

Key factors that affect evidence preservation and investigation time:

- ✓ 1. How logging is done
- ✓ 2. What is logged
- ✓ 3. IDS under use
- ✓ 4. Forensics acquisition (of the evidence)
- ✓ 5. Evidence handling

Concerns with Being a Forensically Ready Organization

- ✓ Digital evidence is required.
- ✓ An organization needs access to the evidence that will be able to support its position.
- ✓ There is always a tendency to focus on containment and recovery.
- ✓ There is a trade-off to be made between recovery and evidence.
- ✓ A lot of information is also lost or discarded.

Benefits of Being a Forensically Ready Organization

1. The ability to gather evidence that can serve in the company's defense if subjected to a lawsuit.
2. Comprehensive evidence gathering can be developed as a deterrent to the insider threat (throwing away potential evidence is simply helping to cover the tracks of a cybercriminal).
3. In case of a major incident, a rapid and efficient investigation can be conducted and actions can be taken with a view to minimal disruption to the business.
4. Reduction in cost and time of an internal investigation through a systematic approach to evidence storage.
5. A structured approach to evidence storage can reduce the costs of any court-ordered disclosure or regulatory or legal need to disclose data (e.g., in response to a request under data protection legislation).
6. Forensics readiness can widen the scope of information security to the wider threat from cybercrime, such as IP protection, fraud or extortion.
7. It demonstrates due diligence and good corporate governance of the company's information assets. It can further demonstrate that regulatory requirements have been met.
8. It can improve and facilitate the interface to law enforcement, if involved.
9. It can improve the prospects for a successful legal action.
10. It can provide evidence to resolve a commercial dispute.
11. It can support employee sanctions based on digital evidence (e.g., proving violation of an Acceptable Usage Policy).

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.
- 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.

Aspects pivotal to a sound 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.

Figure 5 presents the elements that affect an access management framework based on fundamental governance principles. The elements in the figure indicate that a mature access management framework spans across corporate instructions based on organizational standards and guidelines.

Importance of Endpoint Security in Organizations

- People who are out of 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.
- 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.
- 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.
- 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.

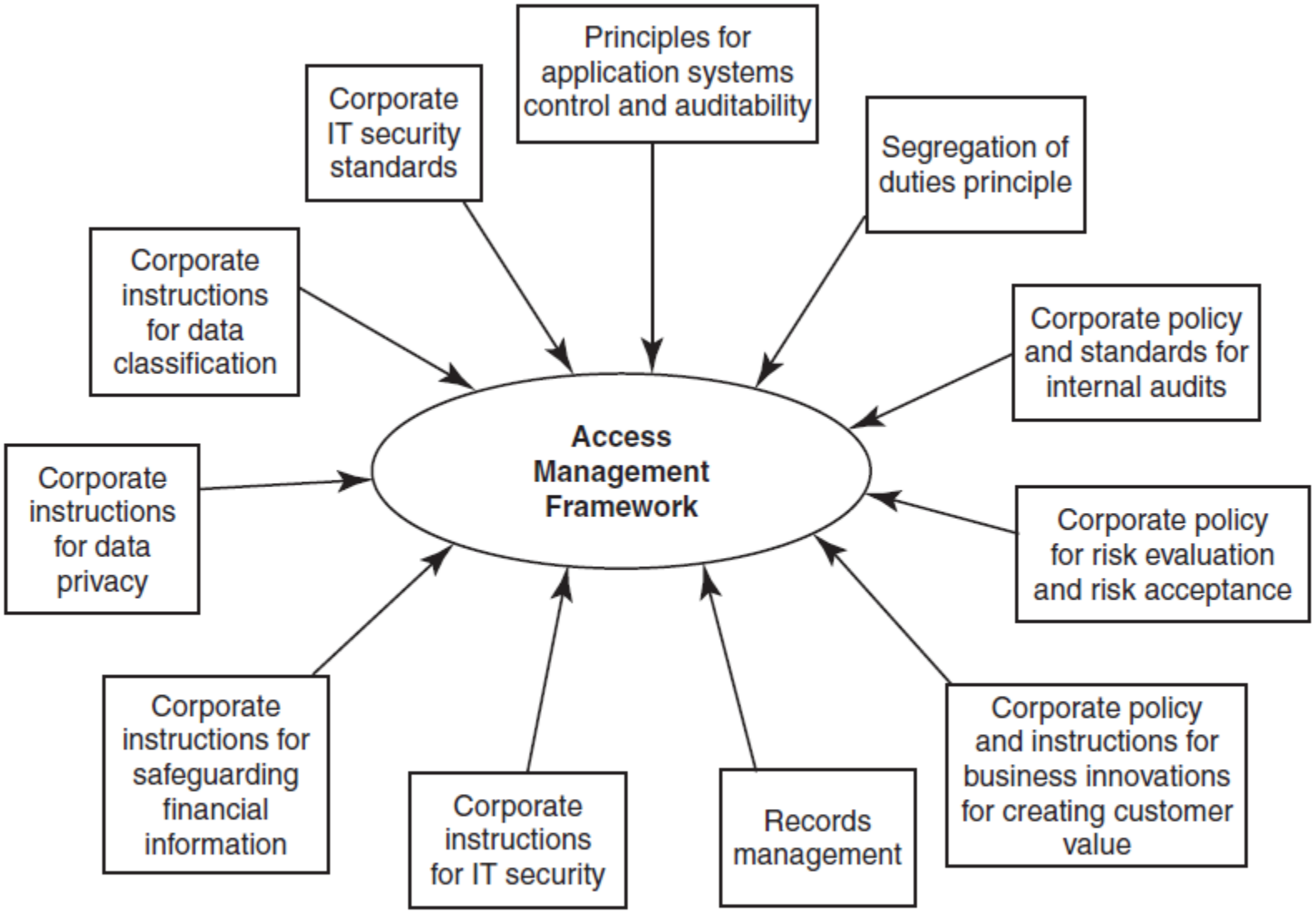


Figure 5 | Access management framework – key elements.

- 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 get quarantined.
- Users of those devices should be provided with direction and resources for updating the device with the necessary patches and security setting.

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