UNIT-5

CYBER SECURITY/CRIME

ORGANIZATONAL IMPLICATIONS

1. What is Cyber Crime ? Give Examples.

"cybercrime (computer crime) is any illegal behavior, directed by means of electronic operations, that targets the security of computer systems and the data processed by them."

A crime committed using a computer and the Internet to steal a person's identity (identity theft) or sell contraband or stalk victims or disrupt operations with malevolent Programs.

Table 1.1 | Cybercrimes/cases registered and persons arrested under IT Act during 2004–2007

Sr. No.	*Crime Heads*	*Cases Registered*				*% Variation in 2007 over 2006*	*Persons Arrested*				*% Variation in 2007 over 2006*
		2004	*2005*	*2006*	*2007*		*2004*	*2005*	*2006*	*2007*	
1	Tampering computer source documents	2	10	10	11	10.0	0	10	8	2	–75
2	Hacking with computer system										
	(i) Loss/damage to computer resource/utility	14	33	25	20	–20.0	31	27	34	25	–26.5
	(ii) Hacking	12	41	34	46	35.3	1	14	29	23	–20.7
3	Obscene publication/transmission in electronic form	34	88	69	99	43.5	21	125	81	86	6.2
4	Failure										
	(i) Of compliance/orders of Certifying Authority	0	1	0	2	—	0	0	0	1	—
	(ii) To assist in decrypting the information intercepted by government agency	0	0	0	2	—	0	0	0	0	—
5	Unauthorized access/attempt to access to protected computer system	0	0	0	4	—	0	0	0	0	—
6	Obtaining licence or digital signature certificate by misrepresentation/suppression of fact	0	0	0	11	—	0	0	0	11	—
7	Publishing false digital signature certificate	0	0	0	0	—	0	0	0	0	—
8	Fraud digital signature certificate	0	1	1	3	200.0	0	3	0	3	—
9	Breach of confidentiality/privacy	6	3	3	9	200.0	7	13	2	3	50.0
10	Other	0	0	0	0	—	0	0	0	0	—
	Total	**68**	**177**	**142**	**207**	**45.8**	**60**	**192**	**154**	**154**	**0.0**

Source: http://www.nasscom.org/download/Cybercrimes in India 2003.pdf (28 February 2009).

1. Cybercrime against individual

- *Electronic mail* (*E-Mail*) *Spoofing and other online frauds*
- *Phishing, Spear Phishing* and its various other forms such as Vishing
- *Spamming*
- *Cyberdefamation*
- *Cyberstalking and harassment*

2.Cybercrime against property

- *Credit card frauds*
- *Intellectual property (IP) crimes:* Basically, IP crimes include software piracy, copyright infringement, trademarks violations, theft of computer source code, etc.
- *Internet time theft:*

3. Cybercrime against organization

- *Unauthorized accessing of computer:* Hacking is one method of doing this and hacking is a punishable offense
- *Password sniffi g*
- *Denial-of-service attacks* (known as DoS attacks
- *Virus attack/dissemination of viruses:*

4.Cybercrime against Society

- *Forgery*
- *Cyber terrorism*
- *Web jacking*

5. Crimes emanating from Usenet newsgroup: By its very nature, Usenet groups may carry very offensive, harmful, inaccurate or otherwise inappropriate material, or in some cases, postings that have been mislabeled or are deceptive in another way.

Therefore, it is expected that you will use caution and common sense and exercise proper judgment when using Usenet, as well as use the service at your own risk.

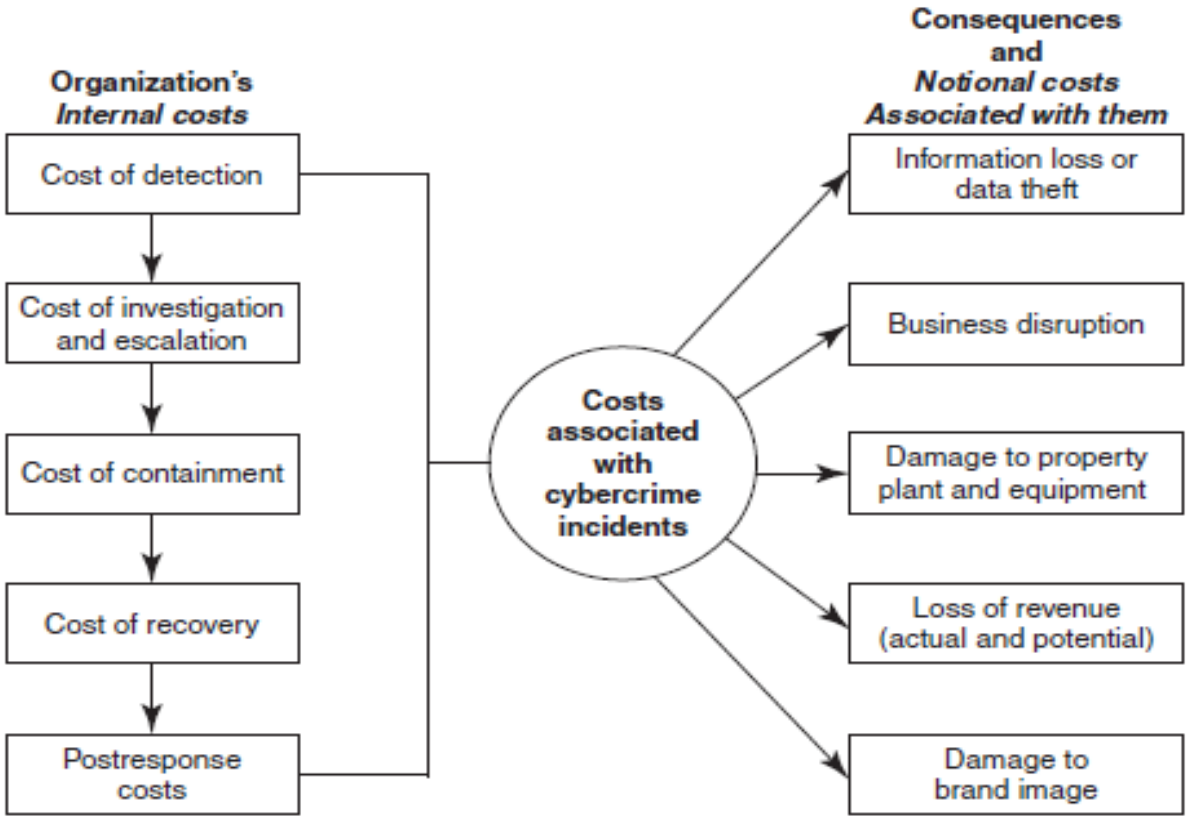
In the global environment with continuous network connectivity, the possibilities for cyber attacks can emanate from sources that are local, remote, domestic or foreign. They could be launched by an individual or a group.

A "security breach" is defined as unauthorized acquisition of data that compromises security, confidentiality or integrity of personal information (PI) maintained by us.

2.Discuss about Cyber Crime Costs

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

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 cyber attacks than any other industry.



igure 9.5 | Cost of cybercrimes.

The internal costs typically involve people costs, overhead costs and productivity losses. The internal costs, shown in Fig. 9.5, are in order from largest to the lowest and that has been supported by the benchmark study mentioned previously:

1. Detection costs (25% – largest).
2. Recovery costs (21%).
3. Post response costs (19%).
4. Investigation costs (14%).
5. Costs of escalation and incident management (12%).
6. Cost of containment (9% – lowest).

The consequences of cybercrimes and their associated costs, mentioned in figure above show a pattern

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%).

There is a subjective element depending on the nature of an organization – for example, revenue costs could be higher for a fully E-Commerce company that purely sells from the Web-based portal, that portal is completely down following a cyber attack.

The benchmark study mentioned at the beginning of this section revealed that the percentage of organizations impacted by various types of cybercrimes show the following distribution:

1. Viruses, worms and Trojans (100%):
2. Malware (80
3. Botnets (73%)
4. Web-based attacks (53%)
5. Phishing and social engineering (47%)
6. Stolen devices (36%)
7. Malicious insiders (29%)
8. Malicious Code (27%)

Now-a-days, cyber crimes do not only confine itself to fraud, cyber bullying, identity thefts but also infringement of copyrights and trademarks of various business and other organization's.

1. Endpoint protection: It is an often ignored area but it is important IP-based printers, although they are passive devices, are also one of the endpoints. Printers are no more just dump devices especially in the network printer era. Many organizations,
which otherwise have reasonably good security practices, tend to completely neglect their network printers

2. Secure coding: These practices are important because they are a good mitigation control to protect organizations from "Malicious Code" inside business applications (especially those applications that are mission critical).

3.HR checks: These are important prior to employment as well as after employment (from malicious insiders' considerations).

4. Access controls: These are *always* important, for example, shared IDs and shared laptops are dangerous. Access privileges should be granted carefully, especially when they involve access to confidential and sensitive information of the organization

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

3.Discuss about Intellectual Property Rights Issues. (IPR)

This intellectual property can include **ideas, inventions, words, slogans, original works of authorship, and any proprietary information**. Intellectual property infringement can also happen through trademark counterfeiting and copyright piracy. This can even threaten the general public.

The advancement in e-commerce and e-business has led to an important concern to the companies and organization's to protect their intellectual property rights online.

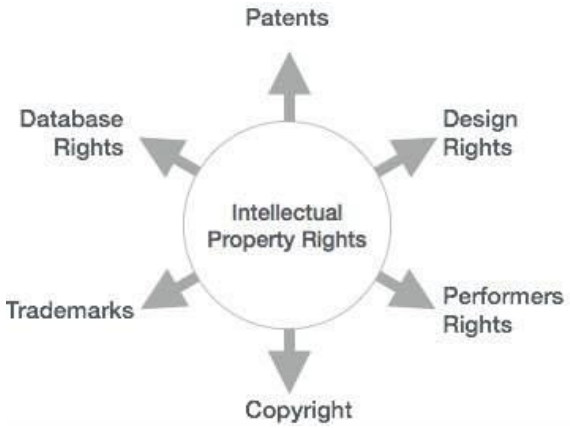
Intellectual Property Rights (IPR) and Cyber Laws cannot be separated, and online content must be protected.

In cyberspace, sometimes private information is shared by a person who is not the owner. Hence, privacy is violated. One makes profit from another person's creation. Those rights are protected under IPR.

Copyright Infringement:

Copyright protection is given to the owner of any published artistic, literary, dramatic, or scientific work over his work to exclude everyone else from using that work on his own name and thereby gain profit from it.

When these copyrights are used by anybody without the permission of the owner, it amounts to infringement of such copyright/ COPYRIGHT VIOLATION.



Copyright Issues In Cyber Space:

Linking:

It allows the user of the website to go to another website on the Internet without leaving that website that he is uses. It is done by clicking on a word or image in one web page. Linking damages the rights or interests of the owner of the webpage

Software Piracy:

It is also covered under Indian Copyright Act . This is knowingly making use on a computer of an infringing copy of a computer programme.
Piracy can be of 3 types: Soft lifting ,Software Counterfeiting,Uploading-Downloading.

Cybersquatting And Trademark Infringement:

Trademark means a mark capable of being represented graphically and which can distinguish the goods or services of one person from those of others and may include shape of goods, their packaging and combination of colours.

Cybersquatting is done when domain names are registered, sold or trafficked-in with the intention to make profit from the goodwill of someone else. It is a punishable.

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 Act 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.

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.

Advantages of Intellectual Property Rights

- Provides exclusive rights to the creators or inventors.
- Encourages individuals to distribute and share information and data instead of keeping it confidential.
- Provides legal defense and offers the creators the incentive of their work.
- Helps in social and financial development.

Cyber Laws are the sole savior to combat cyber-crime. It is only through stringent laws that unbreakable security could be provided to the nation's information. The I.T. Act of India came up as a special act to tackle the problem of Cyber Crime. The Act was sharpened by the Amendment Act of 2008.

Cyber Law also called IT Law is **the law regarding Information-technology including computers and internet**. It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce. ... Intellectual property is a key element of IT law.

Importance of Cyber Law:

- It covers all transaction over internet.
- It keeps eyes on all activities over internet.
- It touches every action and every reaction in cyberspace.

4. Discuss about Web Threats for Organizations:

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 (weather forecasts, stock trading and video conferencing).
- Therefore, cybercriminals find it convenient to use the Net for committing crimes.

Challenges of Organization

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.

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.

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. This threat is more in the case of younger employees; especially in the IT industry where at times they are on the bench.

2. Enforcing "Acceptable Use Policies" is a challenge, especially, in very large, multi-location and 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 the necessary evil in Windows world.

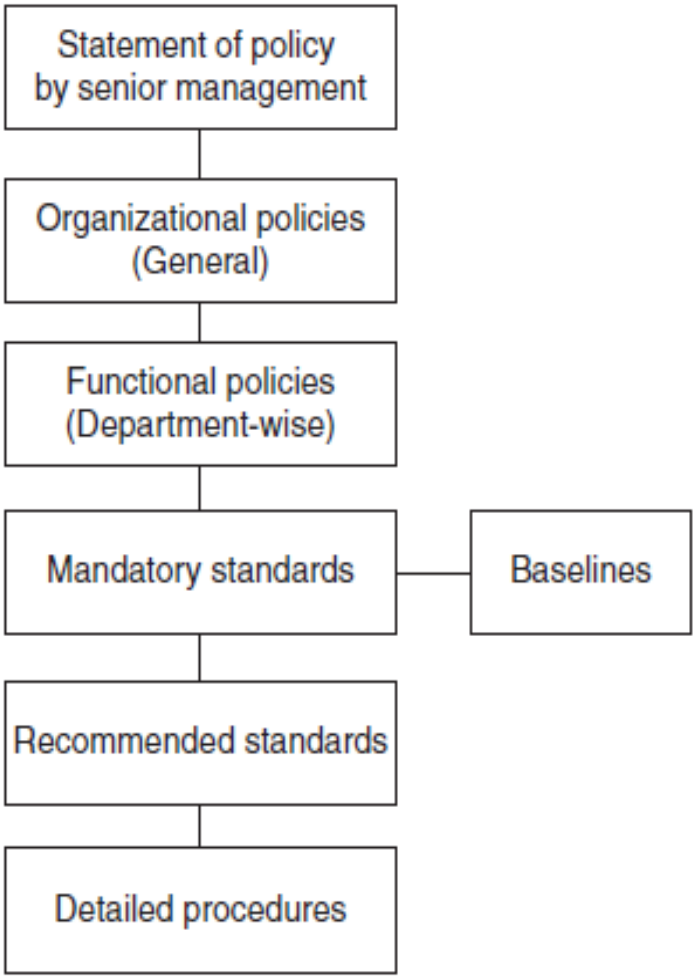
5. Legal and regulatory compliance risks (such as employees visiting inappropriate websites and the accidental disclosure of confidential information online). Laws are getting tough and regulatory compliance pressures are high especially in data breaches and employee privacy matters.

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.

Enforcing Policy Usage in the Organization Figure depicts the policy hierarchy chart. 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.



9. Protecting the organization against Spyware and malware –
Today there are tools from Wenbsense Inc., called Websense Enterprise Edition, meant for content filtering. Remote filtering capabilities are incorporated into the newest versions of Websense. Web filtering and web security software restrict the use of Internet. In References, some useful links are provided for those who are interested in exploring the features of this tool.

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.

Monitoring Internet Surfing does keep the IT department very busy because dealing with the disciplinary issues is a serious drain on management time –

first, you have to constantly monitor; then you have to classify the findings and then you have to report.

Second, you need to hold meetings to discuss the issues; then you need to agree on an action plan and finally you need to report the actions taken.

Therefore, the IT department or whichever department is given the task of monitoring employees' Internet surfing time needs to be empowered with the ability to restrict access to non-work websites. Without this kind of technology, employee's time wasting goes unchecked and policy enforcement becomes much more difficult.

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. Given the nature of security threats today, such a policy is necessary but not sufficient on its own.

Its effective implementation draws from the continuous training to educate users about security policies.

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.

Thus, organizations need to decide what type of access they should provide to employees. Some organizations will want to block non-work sites completely whereas others will want to allow access to some sites or within certain time limits.

5. What is Social Media Marketing and discuss about Security Risks and Perils for Organizations

Social media marketing includes activities like posting text and image updates, videos, and other content that drives audience engagement, as well as paid social media advertising.

The term **social media marketing** (**SMM**) refers to the use of social media and social networks to market a company's products and services.

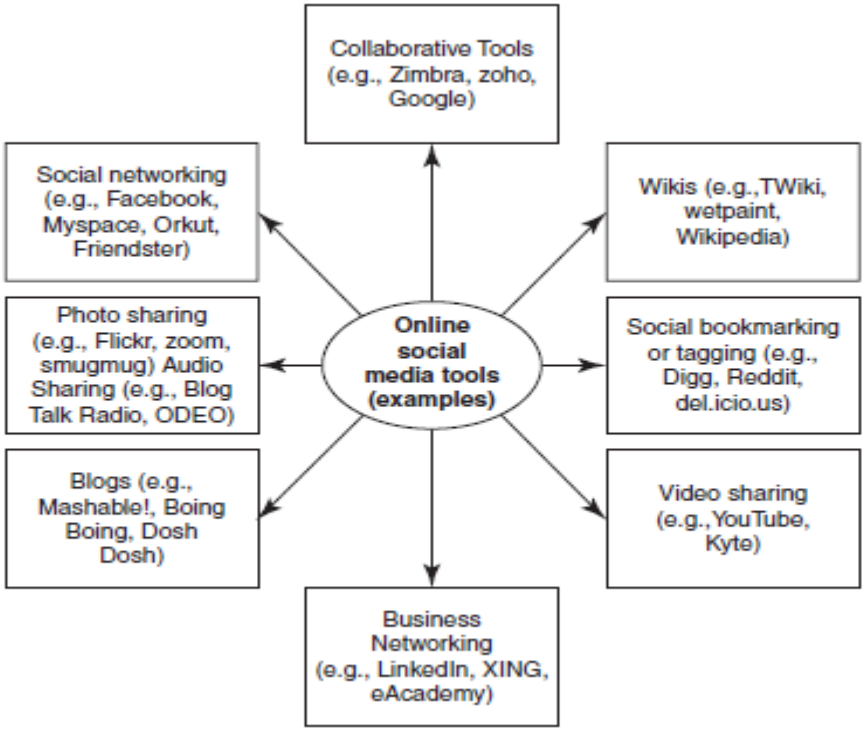
According to fall 2009 survey by marketing professionals, usage of social media sites by large business-to-business (B2B) organizations shows the following:

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. MySpace is used by 6% of the organizations.

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.

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." The phenomenon called "social media marketing" and the reasons why it is used is worth understanding.

"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. Figure shows different types of social media tools.



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:

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 as user profile data, which can be used to target a specific set of users for advertising

As the Web continues to grow and evolve with the adoption of Web 2.0 applications, virus outbreaks and other forms of web-borne threats known as “malware” continue to grow as well.

It is good to use multi-layered solutions that have an array of analysis techniques (e.g., antivirus signatures and network intelligence heuristics, behavioral analysis, etc. that may help real-time analysis of URLs) including real-time scanning. There are many web security solution vendor companies that offer specialized solutions that can be located on the Internet.

Organization measures to reduce threats.

1. 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.

2. Organizations need to educate their employees about the risks associated with the use of online social media tool.

3. 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.

4. Providing continuous information about new security threats and maintaining rules of conduct can enhance employee awareness.

5. On the basis of staffing budget available in the organization, it is worth exploring appointment of a social media expert within the company. Such an expert can serve as a permanent contact for employees for their questions on social media marketing tool usage especially when the staff is engaged in marketing activities.

6. Network security administrators need to remain up to date about the most recent risks on the Web. There is a strong need to establish firm processes that are systematically linked to daily workflows. Such processes should be easy to implement and audit.

7. 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.

8. With organization guidelines available, network administrators find it easier to define the network domain as well as the applications that can be accessed by specific people at specific times. For this, you need to establish the "need-based access policy." Once you have this in place, 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. Thus, strong access control policies and monitoring of user accesses in an ongoing manner is essential.

9. Blocking the infected websites is another necessary activity.

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. Impersonation and identity theft.

In a way, social computing is related to social media marketing because business leaders in product development, marketing and sales view social computing as an integral part of the evolving enterprise channel strategy.

The CIOs, however, see it as a source of many security and privacy risks. Recommendation is to take due care while using social computing as a channel strategy for communicating with internal or external stakeholders such as employees, customers and suppliers.

The best defenses against social media hacking are strong passwords and social media monitoring tool

Brands like Google, Alibaba, L'Oreal, H&M, and Mashable, trust Keyhole's analytics. Keyhole is a social media analytics solution allowing you to track hastags and keywords to monitor relevant conversations online.

Keyhole's social analytics dashboard gives you an instant rundown of what your brand's health looks like.

Brandwatch is a social listening & analytics tool that helps you dig out relevant data from blogs, forums, as well as social media and news or review sites. Basically, this tool tells you what/how your customers talk about your brand online.

Glean.info is a market intelligence and social media monitoring tool that gets audience data from social media sites, online news, blogs, message boards, forums, and photo/video sharing sites.

Similar to Keyhole and BrandWatch, this tool also lets you see your share of voice on social. That is, the percentage of your brand's mentions against that of your competitor's.

The evident lack of **privacy on social media** makes it important to protect your online privacy before you share anything on any social media platform

1. **Read and Understand the Privacy Terms**
2. **Site Features**
3. **Adjust your Privacy Settings**
4. **Biographical Information**
5. **Account Information**
6. **Friends or Contacts**
7. **Turn Off Your Location**
8. **Be careful about posting photos online**

6.Discuss about Digital Forensics.

Digital forensics is a branch of forensic science that **focuses on identifying, acquiring, processing, analysing, and reporting on data stored electronically**. Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations.

Digital forensics is **the scientific acquisition, analysis, and preservation of data contained in electronic media whose information can be used as evidence in a court of law**. The practice of digital forensics can be a career unto itself, and often

Some of the main types include the following:

Database forensics. The examination of information contained in databases, both data and related metadata.

- Email forensics. ...
- Malware forensics. ...
- Memory forensics. ...
- Mobile forensics. ...
- Network forensics.

a digital forensic investigator's role is to recover data like documents, photos, and emails from computer hard drives and other data storage devices, such as zip and flash drives, with deleted, damaged, or otherwise manipulated.

Steps of Digital Forensics

In order for digital evidence to be accepted in a court of law, it must be handled in a very specific way so that there is no opportunity for cyber criminals to tamper with the evidence.

1. Identification

First, find the evidence, noting where it is stored.

2. Search and Seizure

Recognized the evidence and seize it.

3. Preservation

Next, isolate, secure, and preserve the data. This includes preventing people from possibly tampering with the evidence.

4. Analysis

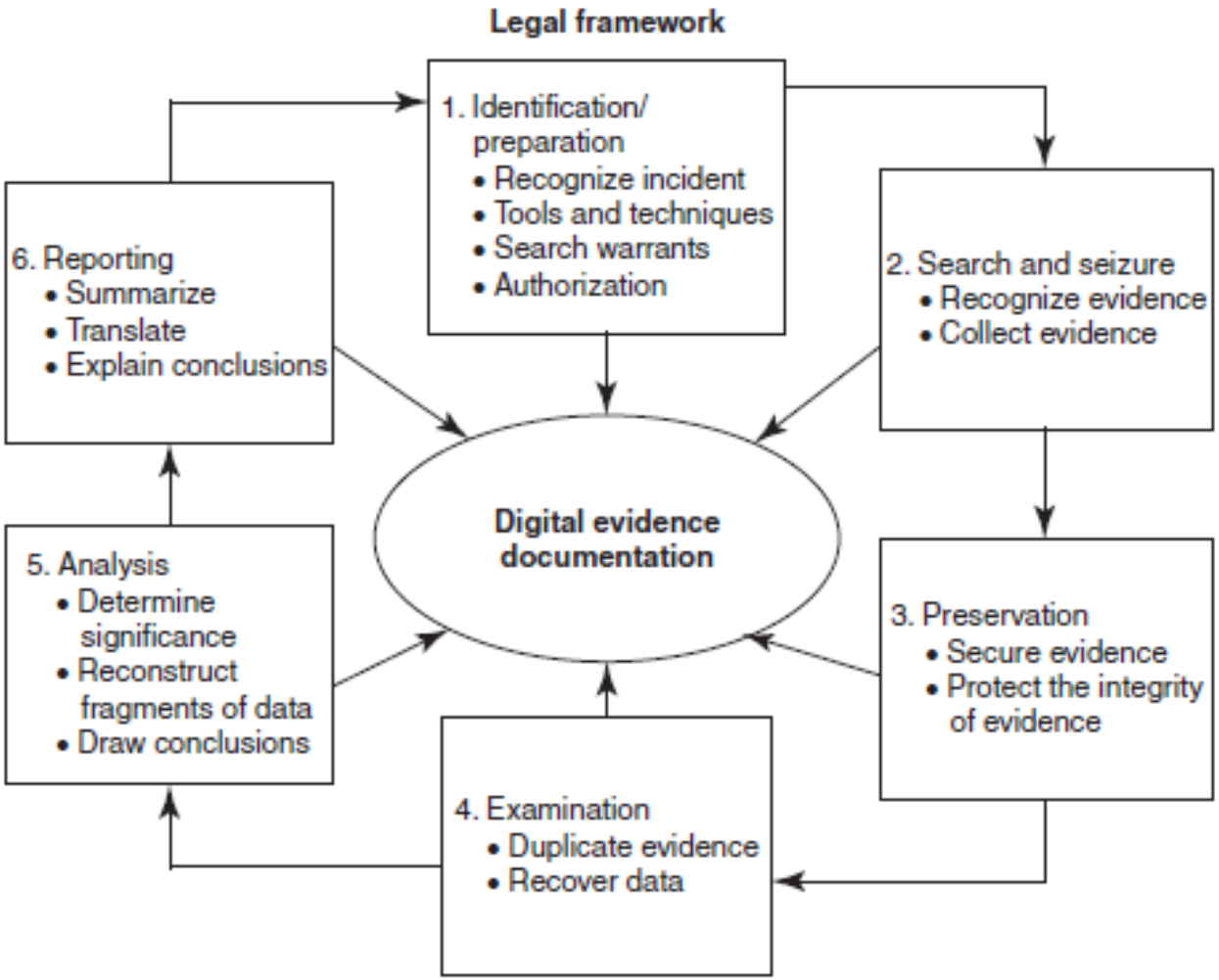
Next, reconstruct fragments of data and draw conclusions based on the evidence found.

5. Documentation

Following that, create a record of all the data to recreate the crime scene.

6. Presentation

Lastly, summarize and draw a conclusion.


Legal framework
1. Identification/ preparation
• Recognize incident
• Tools and techniques
• Search warrants
• Authorization
2. Search and seizure
• Recognize evidence
• Collect evidence
3. Preservation
• Secure evidence
• Protect the integrity of evidence
4. Examination
• Duplicate evidence
• Recover data
5. Analysis
• Determine significance
• Reconstruct fragments of data
• Draw conclusions
6. Reporting
• Summarize
• Translate
• Explain conclusions
Digital evidence documentation

For businesses, Digital Forensics is an important part of the Incident Response process. Forensic Investigators identify and record details of a criminal incident as evidence to be used for law enforcement. Rules and regulations surrounding this process are often instrumental in proving innocence or guilt in a court of law.

Eventually, digital forensic tools were created to observe data on a device without damaging it. Presently, **digital forensic tools can** be classified as digital forensic open source tools, digital forensics hardware tools, and many others.

The Sleuth Kit (earlier known as TSK) is a collection of Unix- and Windows-based utilities that extract data from computer systems. It is an **open-source software** that analyzes disk images created by "dd" and recovers data from them. With this software, professionals can gather data during incident response or from live

FTK Imager is an acquisition and imaging tool responsible for data preview that allows the user to assess the device in question quickly. The tool can also create forensic images (copies) of the device without damaging the original evidence.

Xplico is a network forensic analysis tool (NFAT) that helps reconstruct the data acquired using other packet sniffing tools like Wireshark. It is **free and open-source software** that uses Port Independent Protocol Identification (PIPI) to recognize network protocols. The tool is built on four key components: Decoder Manager, IP Decoder, Data Manipulators, and Visualization System.

The following is a list of scenarios where digital evidence would become necessary:

- Disputed transactions
- Allegations of employee misconduct
- Showing legal and regulatory compliance
- Avoidance of negligence and breach-of-contract charges
- Assisting law enforcement investigations
- Meeting disclosure requirements in civil claims
- Supporting insurance claims when a loss occurs

Several open-source tools are available to conduct an analysis of open ports, mapped drives (including through an active VPN connection) and open or mounted encrypted files (containers) on the live computer system.

Utilizing open-source tools and commercially available products, it is possible to obtain an image of these mapped drives and the open encrypted containers in an unencrypted format. Open-source forensics tools for PCs include Knoppix and Helix by US e-fense Inc.

These are Unix-based tools used in Linux environment. Commercial imaging tools include Access Data's Forensics Toolkit and Guidance Software's EnCase application.

The above-mentioned open-source tools mentioned can also scan RAM and Registry information to show recently accessed Web-based E-Mail sites and the login/password combination used.

7. Discuss about Protecting people privacy in the organization

Data privacy generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. This personal information can be one's name, location, contact information, or online or real-world behavior

Businesses and other organizations are increasingly aware of the serious adverse consequences of disclosure of their data. The threat posed by criminals, computer hackers, and other malicious parties has been widely documented.

Why Privacy ?

#1. Privacy rights prevent the government from spying on people (without cause)
#2. Privacy rights keep groups from using personal data for their own goals
#3. Privacy rights help ensure those who steal or misuse data are held accountable
#4. Privacy rights help maintain social boundaries
#5. Privacy rights help build trust
#6. Privacy rights ensure we have control over our data
#7. Privacy rights protect freedom of speech and thought
#8. Privacy rights let you engage freely in politics
#9. Privacy rights protect reputations
#10. Privacy rights protect your finances

Best Practices of Privacy

1. Practice minimal data collection

A rule of thumb when collecting data is to only collect what you need. For example, if you don't need to know someone's date of birth or their name prefix, e.g. Mr., Ms., Miss, then don't collect it. This helps to save you bandwidth in protecting that information, too.

2. Make it a two-way conversation

Privacy can become a way to engage with your customers and show them you respect their data. GDPR sets out to make the use of consent an integral part of data collection and use. When you design your user experience and associated UI, build in consent models whenever you collect or use data.

3. Practice robust data security

Privacy covers many areas, including the ability to choose to share data. However, to apply these choices and to protect the underlying data, security measures need to be implemented.

4. Encourage education and awareness

Education on security and privacy issues is not just about your employees becoming security-aware. You should also endeavor to educate your customers about security and privacy. This can include regular advisories on patching, protection of credentials, phishing and so on.

5. Create achievable policies and SLAs with third parties

Privacy is a whole-system effort. Any touch point within your company, across your services, and in the way you process data and manage customers has a potential impact on privacy. Security and privacy policies MUST reach out to the extended data and vendor ecosystem.

6.You should integrate training on data privacy into your general training program, and it should be part of the onboarding process for new staff.

7.Make sure that you take advantage of the free security tools that are out there. This includes encrypted storage solutions, password managers, and VPNs. These small tools can dramatically decrease your vulnerability to attack, and are easy to use and install.

8.Monitor your network for suspicious activity, so that you can catch on to an attack early enough to reduce the damage.

9.Implement the zero trust model. “Zero Trust restricts access to the entire network by isolating applications and segmenting network access based on user permissions, authentication and user verification. With Zero Trust policy enforcement and protection are easily implemented for all users, devices, applications and data, regardless of where users are connecting from. This user-centric approach makes the verification of authorized entities mandatory, not optional. This ‘trust, but verify’ mindset is absolutely essential for today’s organizations.”

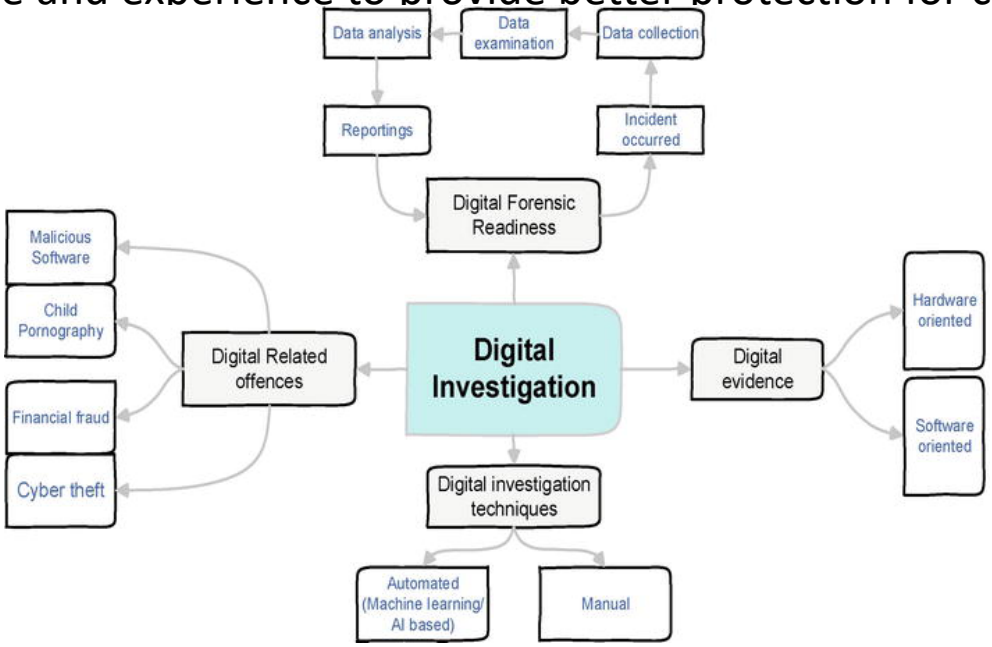
- Develop and implement policies and practices for handling personal information and make this information available to the public on request
- Obtain consent from the individual whose personal information is collected, used or disclosed
- Obtain the individual's consent before or at the time of collection and when a new use is identified
- Before or at the time of collection, inform the individual of the purposes for collecting personal information
- Destroy, erase or make anonymous any personal information as soon as it is no longer required for a legal or business purpose
- Make reasonable efforts to ensure that the personal information you collect is accurate and complete
- Make reasonable security arrangements to protect personal information under your control, including physical measures, technical tools and organizational controls where appropriate
- Safeguard personal information from unauthorized access, collection, use, disclosure, copying, modification or disposal by individuals from within and outside your organization

8. Discuss about Digital Forensics best practices for organizations

Computer Forensics is a new discipline in computer science that deals with the gathering, retrieving and evaluating of electronic data, for the purpose of stopping and preventing computer fraud, or gather and preserve digital evidence for a criminal investigation, or to recover data accidentally lost or deleted.

Computer forensics is an approach or method used by investigators to identify the source of an attack on computers and data-related resources and systems.

- Identification of unauthorized activities and activities that occurred.
- Gathering, processing, storing and preserving evidence that might be introduced in the court of law.
- To use that knowledge and experience to provide better protection for computer systems.



Best practices for digital forensic investigations, which are:

Shutting down the system: The system under investigation must be shut down or powered down as quickly as possible. Depending on the computer operating system this process might involve pulling the plug or shutting down a networked computer using relevant operating systems commands.

Documentation of the computer hardware configuration: It is very crucial to document all the system hardware components, where they were located and how they were connected. This can be done by taking pictures from different angles and labeling all wires and system components and devices so that the original configuration of the system can be restored when needed.

Securing the computer system: The computer under question and all hardware, software and all other resources that belong to the system under investigation should be treated as evidence, therefore it should be stored out of reach of all outsiders and not left unattended.

Backup all storage devices: The system should not be used or operated and no evidence can be processed until at least two bit stream backup (exact copies) have been made on all disk drives and other storages devices. The original evidence should not be touched at all. It can only be introduced in a court of law in the form of admissible evidence. Preservation of evidence is the most important and crucial factor to consider.

Authentication of the data on all storage devices: Investigators need to prove that collected evidence is not altered or changed by any means. Such proof can be provided by authenticating the data with high level accuracy that is beyond question.

Develop a list of search words: Due to the fact that modern data storage devices are so voluminous, it is impossible to perform a manual viewing and evaluation of all data files on system data storage devices. High technology and modern automated forensic text search tools are used to find relevant evidence.

Evaluation of file slack: File slack is a data storage which is beyond the reach or view of computer users and operators. File slack is a source of significant security leads. In order to view and evaluate file slack, special forensic tools are required. File slack can provide wealth of information and investigative leads such as relevant search key words.

Erased files: As is well known the delete command or function in most of operating systems does not permanently erase file names or content, the storage space associated with such files becomes unallocated and available to be overwritten by new files. This unallocated space can be a source of significant leads because it contains erased files and file slack associated with

File attributes: It is very important to document all file attributes such as file names, creation dates, last modified, etc. From file attributes, with the help of special forensic tools, a time line of computer usage can be obtained which is crucial from an evidence standpoint.

Identification of data and data storage types: In case data stored in storage devices are encrypted, compressed or stored in graphic files, text search programs cannot identify these types of files. As a result investigators need to perform manual evaluations of these files, not only that but in the case of encrypted files much more technical work is required.

Program functionality: Forensic experts need to investigate all installed software programs, applications and tools. Investigators need to identify the purpose of all installed software. This can be achieved by running and executing these programs.

Documentation of findings: As was stated earlier, it is essential to treat all findings as evidence. Therefore, investigators need to document all their findings along with date, time, etc, software programs and tools used in investigations.

Finally, after applying the above illustrated points, investigators need to prepare the forensic report. The forensic report is a report of all the meaningful data that must satisfy the forensic request. This report must be prepared and organized in a way that makes it understandable and usable by the requester.

In other words managerial implications are factors that help in talking right decisions at right times, e.g., whether to go ahead with a case, how much to invest and etc. key elements of digital forensics managerial implications are:

Investigator's Skills: The investigation process requires far more skill than just the ability to retrieve data, especially when a criminal case is involved. That is when the investigator will need to testify as to what they did to the system under question. Also the court will need to know investigators level of education, training and experience in the field of computer and digital forensics. Therefore it is very important that investigators conducting the forensic investigation are properly skilled in this trade.

Forensic Tools: The authenticity and reliability of the collected evidence depends to great extent on the used forensic tools. If used tools are not reliable, the evidence produced by these tools will not be considered reliable. Hence the use of certified tools is a decisive factor for the whole investigation process.

Return on Investment: It is crucial to consider return of investment carefully in all phases of the whole investigation process especially if the requester is considering submitting the case to a court of law. Also it is important for investigators as well as the requester to decide when to stop the investigation process.

Computer Crimes and the Law: Computer forensics is new science and hence the laws associated with this science and all digital crimes are evolving in most countries. Different countries are developing different rules according to many factors; one of these factors is cultural. There is no standard or agreed on set of rules between different countries. Therefore, it is very important and crucial for investigators to be familiar with the rules and regulations of countries involved in the investigations and have sufficient knowledge that enables them to handle the investigation process according to the forensic investigation laws of these countries.