

# What is Security?

Security according to a child of 10 years old



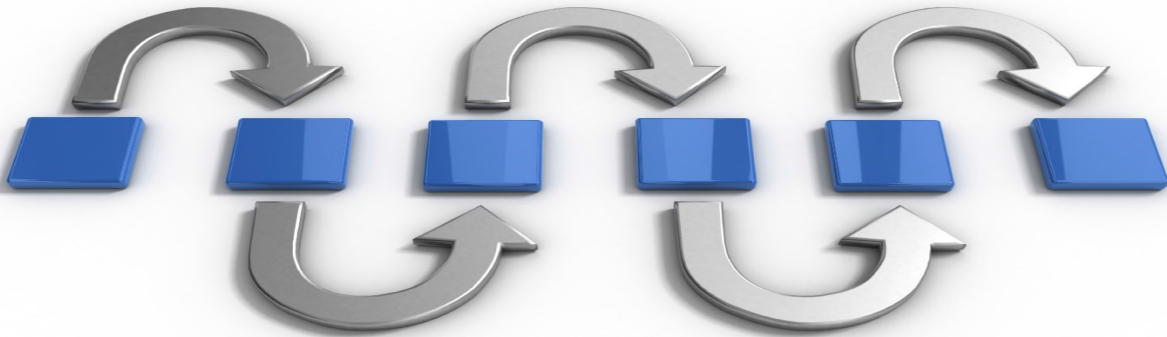
Security According to Junior High School ICT teacher



Security is a process, not an end state.



Security is the process of maintaining an acceptable level of perceived risk.



No organization can be considered "secure" for any time beyond the last verification of adherence to its security policy.

*If your manager asks, "Are we secure?"*

*you should answer, "Let me check."*

*If he or she asks, "Will we be secure tomorrow?"*

*"you should answer, "I don't know."*

Such honesty will not be popular, but this mind-set will produce greater success for the organization in the long run.

## Meaning of the Word CYBER

It is a combining form relating to information technology, the Internet, and virtual reality.



## Cybersecurity Fundamentals – Introduction to Cybersecurity

Adoption of Internet by businesses and enterprises has made mobile-banking, online shopping, and social networking possible. Whilst it has opened up a lot of opportunities for us, its not altogether a safe place because its anonymity also harbors cybercriminals.

### What is cybersecurity?

Cybersecurity is the body of technologies, processes, and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. It may also be referred to as **information technology security**.



The term cybersecurity refers to techniques and practices designed

to protect digital data. The data that is stored, transmitted or used on an information system. After all, that is what criminal wants, *data*. The network, servers, computers are just mechanisms to get to the data. Effective cybersecurity reduces the risk of cyber-attacks and protects organizations and individuals from the unauthorized exploitation of systems, networks, and technologies.

Robust cybersecurity implementation is roughly based around three key terms: *people, processes, and technology*. This three-pronged approach helps organizations defend themselves from both highly organized attacks and common internal threats, such as accidental breaches and human error.

The attacks evolve every day as attackers become more inventive, it is critical to properly define cybersecurity and understand cybersecurity fundamentals.

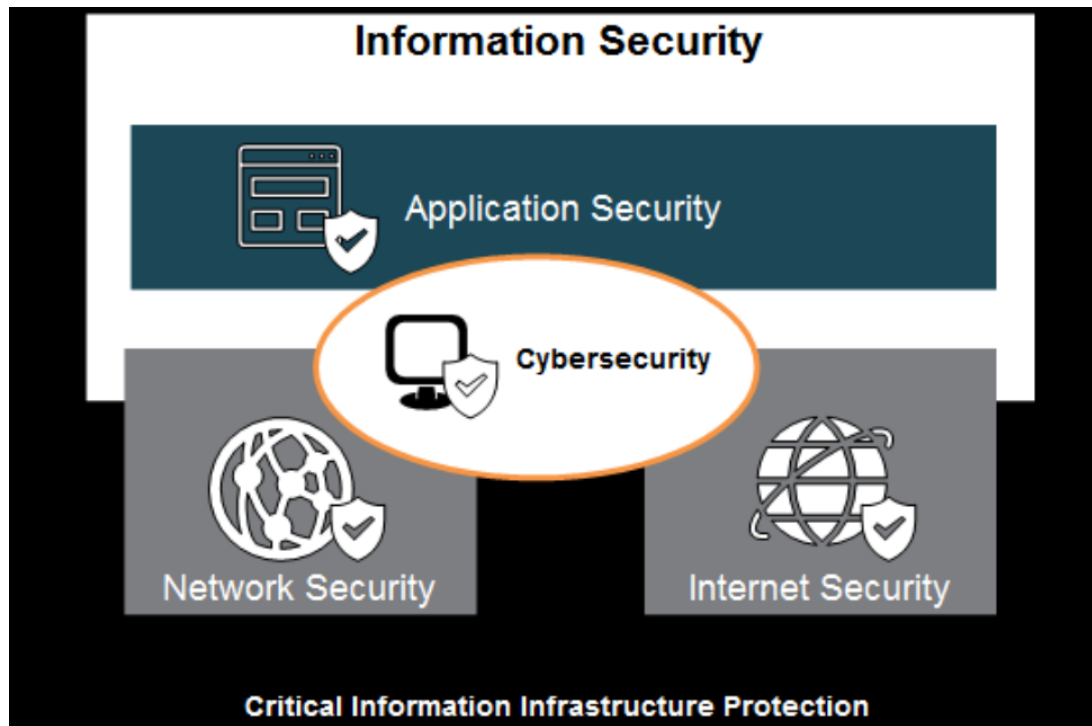
Cyber security encompasses all aspects of security viz., Physical, Technical, Environmental, Regulations and Compliance including Third Parties involved in delivering an objective

With an increasing amount of people getting connected to Internet, the security threats that cause massive harm are increasing also

Major areas covered in cyber security are:







1) Application Security: Application security encompasses measures or counter-measures that are taken during the development life-cycle to protect applications from threats that can come through flaws in the application design, development, deployment, upgrade or maintenance. Some basic techniques used for application security are: a) Input parameter validation, b) User/Role Authentication & Authorization, c) Session management, parameter manipulation & exception management, and d) Auditing and logging.

2) Information Security: Information security protects information from unauthorized access to avoid identity theft and to protect privacy. Major techniques used to cover this are: a) Identification, authentication & authorization of user, b) Cryptography.

3) Disaster recovery: Disaster recovery planning is a process that includes performing risk assessment, establishing priorities, developing recovery strategies in case of a disaster. Any business should have a concrete plan for disaster recovery to resume normal business operations as quickly as possible after a disaster.



4) Network Security: Network security includes activities to protect the usability, reliability, integrity and safety of the network. Effective network security targets a variety of threats and stops them from entering or spreading on the network. Network security components include: a) Anti-virus and anti-spyware, b) Firewall, to block unauthorized access to your network, c) Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks, and d) Virtual Private Networks (VPNs), to provide secure remote access.

5) Internet Security - measures to protect data during their transmission over a collection of interconnected networks

## The history of Cybersecurity

About forty years ago words like *worms*, *viruses*, *trojan-horse*, *spyware*, *malware* weren't even a part of conventional information technology (IT) vocabulary. Cybersecurity only came into existence because of the development of viruses. But how did we get here?

In 1969, **Leonard Kleinrock**, professor of UCLA and student, **Charley Kline**, sent the first electronic message from the UCLA SDS Sigma 7 Host computer to Bill Duvall, a programmer, at the Stanford Research Institute. This is a well-known story and a moment in the history of a digital world. The sent message from the UCLA was the word "login." The system crashed after they typed the first two letters "lo." Since then, this story has been a belief that the programmers typed the beginning message "**lo and behold.**" While factually believed that "**login**" was the intended message. Those two letters of messages were changed the way we communicate with one another.

The history of cybersecurity began as a research project. In the 1970's, Robert Thomas, a researcher for BBN Technologies in Cambridge, Massachusetts, created the first computer "worm". It was called *The Creeper*. The Creeper, infected computers by hopping from system to system with the message "*I'M THE CREEPER: CATCH ME IF YOU CAN.*" Ray Tomlinson, the inventor of email, created a replicating program called *The*



*Reaper*, the first antivirus software, which would chase Creeper and delete it.

Late in 1988, a man named Robert Morris had an idea: he wanted to test the size of the internet. To do this, he wrote a program that went through networks, invaded Unix terminals, and copied itself. The Morris worm was so aggressive that it slowed down computers to the point of being unusable. He subsequently became the first person to be convicted under Computer Fraud and Abuse Act.

From that point forward, viruses became deadlier, more invasive, and harder to control. With it came the advent of cyber security.

## Objectives of cyber security.

Our world today is ruled by technology and we can't do without it at all. From booking our flight tickets, to catching up with an old friend, technology plays an important role in it.

However, the same technology may expose you when it's vulnerable and could lead to loss of essential data.

Cyber security, alongside physical commercial security has thus, slowly and steadily, become one of the most important topics in the business industry to be talked about.

Cyber security is necessary since it helps in securing data from threats such as data theft or misuse, also safeguards your system from viruses.

Cyber security becomes important as Business are being carried now on Network of Networks.

Computer networks have always been the target of criminals, and it is likely that the danger of cyber security breaches will only increase in the future as these networks expand, but there are sensible precautions that organizations can take to minimize losses from those who seek to do harm.

## Why is cyber security important?

We live in a digital era which understands that our private information is more vulnerable than ever before. We all live in a world which is



networked together, from internet banking to government infrastructure, where data is stored on computers and other devices. A portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences.

Cyber-attack is now an international concern and has given many concerns that hacks and other security attacks could endanger the global economy. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cybersecurity describes to protect that information and the systems used to process or store it.

As the volume of cyber-attacks grows, companies and organizations, especially those that deal information related to national security, health, or financial records, need to take steps to protect their sensitive business and personal information.

Listed below are the reasons why cyber security is so important in what's become a predominant digital world:

- With each passing year, the sheer volume of threats is increasing rapidly. *According to the report by McAfee, cybercrime now stands at over \$400 billion, while it was \$250 billion two years ago.*
- Cyber attacks can be extremely expensive for businesses to endure. In addition to financial damage suffered by the business, a data breach can also inflict untold reputational damage.
- Cyber-attacks these days are becoming progressively destructive. Cybercriminals are using more sophisticated ways to initiate cyber attacks.
- Regulations such as GDPR are forcing organizations into taking better care of the personal data they hold.





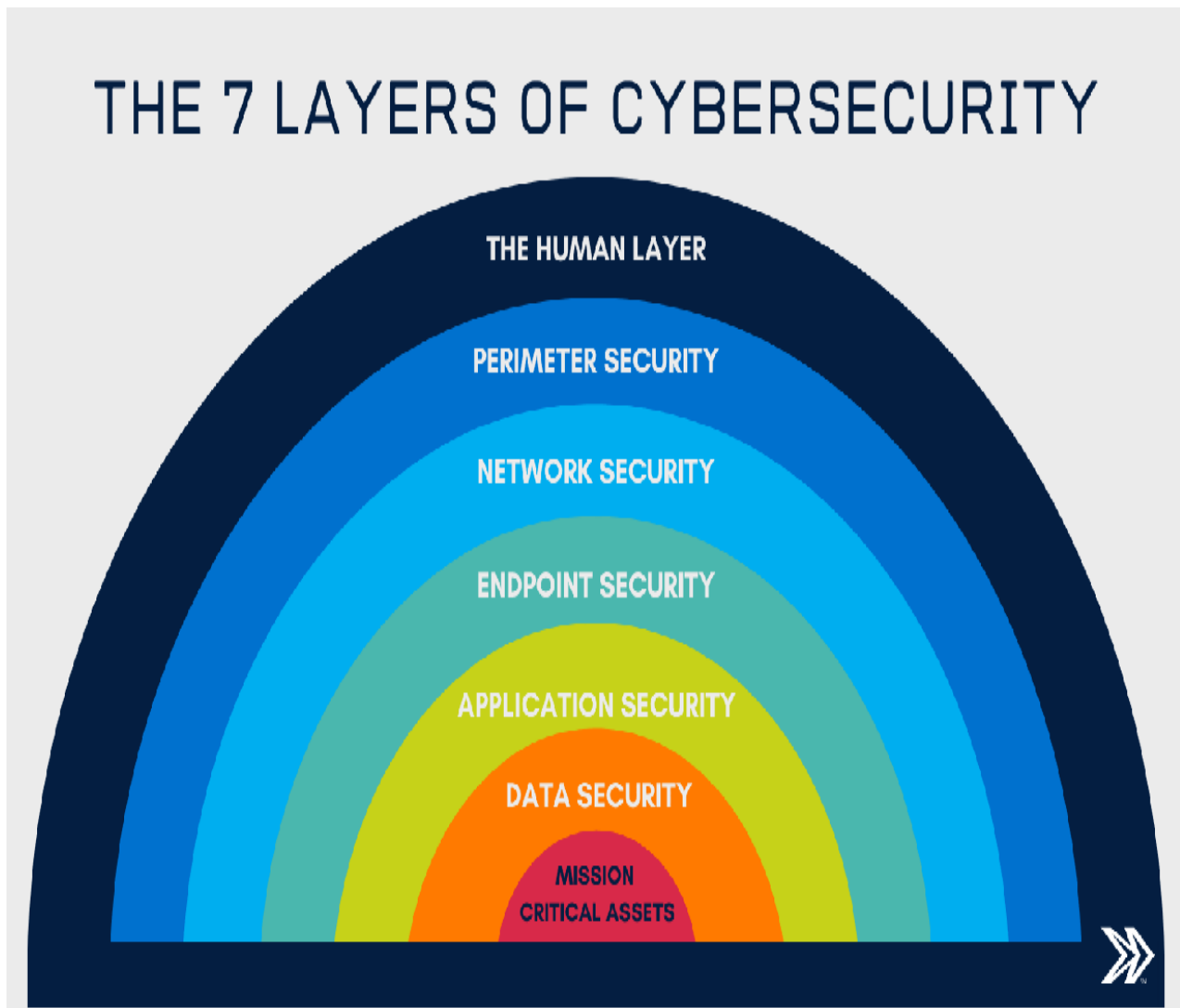
### *The golden age of Hackers – What is Cybersecurity – Edureka*

It can be rightfully said that today's generation lives on the internet, and we general users are almost ignorant as to how those random bits of 1's and 0's reach securely to our computer. For a hacker, it's a golden age. With so many access points, public IP's and constant traffic and tons of data to exploit, black hat hackers are having one hell of a time exploiting vulnerabilities and creating malicious software for the same. Above that, cyber attacks are evolving by the day. Hackers are becoming smarter and more creative with their malware and how they bypass virus scans and firewalls still baffles many people.

Therefore there has to be some sort of protocol that protects us against all these cyber attacks and make sure our data doesn't fall into the wrong hands. This is exactly why we need cybersecurity.



## The 7 Layers of Cyber security



The 7 layers of cybersecurity should center on the mission critical assets you are seeking to protect.

1. **Mission Critical Assets** – This is the data you need to protect
2. **Data Security** – Data security controls protect the storage and transfer of data.
3. **Application Security** – Applications security controls protect access to an application, an application's access to your mission critical assets, and the internal security of the application.
4. **Endpoint Security** – Endpoint security controls protect the connection between devices and the network.



5. **Network Security** – Network security controls protect an organization's network and prevent unauthorized access of the network.
6. **Perimeter Security** – Perimeter security controls include both the physical and digital security methodologies that protect the business overall.
7. **The Human Layer** – Humans are the weakest link in any cyber security posture. Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

## Vulnerability

Vulnerability is a weakness which allows an attacker to reduce a system's information assurance.

Vulnerability is the intersection of three elements:

1. A system susceptibility or flaw,
2. Attacker access to the flaw, and
3. Attacker capability to exploit the flaw.

To exploit vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness.

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems.

### What is the source of a vulnerability?

- Bad software (or hardware)
- Bad design, requirements
- Bad policy/configuration
- System Misuse
  - unintended purpose or environment
  - E.g., student IDs for liquor store

### Vulnerabilities:

They make threat outcomes possible and potentially even more





dangerous. A system could be exploited through a single vulnerability, for example, a single SQL Injection attack could give an attacker full control over sensitive data. An attacker could also *chain* several exploits together, taking advantage of more than one vulnerability to gain more control.

Examples of common vulnerabilities are [SQL Injections](#), [Cross-site Scripting](#), server misconfigurations, sensitive data transmitted in plain text, and more.

**SQL Injection:** SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database. An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities. The OWASP organization (Open Web Application Security Project) lists injections in their [OWASP Top 10 2017](#) document as the number one threat to web application security.

Injection attacks refer to a broad class of attack vectors. In an injection attack, an attacker supplies untrusted input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program.

Injections are amongst the oldest and most dangerous attacks aimed at web applications. They can lead to data theft, data loss, loss of data integrity, denial of service, as well as full system compromise. The primary reason for injection vulnerabilities is usually insufficient user input validation.

This attack type is considered a major problem in web security. It is listed as the number one web application security risk in the [OWASP Top](#)



10 – and for a good reason.

## Types of Injection Attacks

SQL injection (SQLi) and Cross-site Scripting (XSS) are the most common injection attacks but they are not the only ones. The following is a list of common injection attack types.

<b>Injection attack</b>	<b>Description</b>	<b>Potential impact</b>
<b>Code injection</b>	The attacker injects application code written in the application language. This code may be used to execute operating system commands with the privileges of the user who is running the web application. In advanced cases, the attacker may exploit additional privilege escalation vulnerabilities, which may lead to full web server compromise.	Full system compromise
<b>CRLF injection</b>	The attacker injects an unexpected CRLF (Carriage Return and Line Feed) character sequence. This sequence is used to split an HTTP response header and write arbitrary contents to the response body. This attack may be combined with Cross-site Scripting (XSS).	Cross-site Scripting (XSS)
<b>Cross-site Scripting (XSS)</b>	The attacker injects an arbitrary script (usually in JavaScript) into a legitimate website or web application. This script is then executed inside the victim's browser.	<ul style="list-style-type: none"><li>• Account impersonation</li><li>• Defacement</li><li>• Run arbitrary JavaScript in the victim's browser</li></ul>
<b>Email Header Injection</b>	This attack is very similar to CRLF injections. The attacker sends IMAP/SMTP commands to a mail server that is not directly available via a web application.	<ul style="list-style-type: none"><li>• Spam relay</li><li>• Information disclosure</li></ul>
<b>Host</b>	The attacker abuses the implicit trust of the	<ul style="list-style-type: none"><li>• Password-reset</li></ul>



<b>Injection attack</b>	<b>Description</b>	<b>Potential impact</b>
<b>Header Injection</b>	HTTP Host header to poison password-reset functionality and web caches.	<ul style="list-style-type: none"> <li>poisoning</li> <li>• Cache poisoning</li> </ul>
<b>LDAP Injection</b>	The attacker injects LDAP (Lightweight Directory Access Protocol) statements to execute arbitrary LDAP commands. They can gain permissions and modify the contents of the LDAP tree.	<ul style="list-style-type: none"> <li>• Authentication bypass</li> <li>• Privilege escalation</li> <li>• Information disclosure</li> </ul>
<b>OS Command Injection</b>	The attacker injects operating system commands with the privileges of the user who is running the web application. In advanced cases, the attacker may exploit additional privilege escalation vulnerabilities, which may lead to full system compromise.	<ul style="list-style-type: none"> <li>Full system compromise</li> </ul>
<b>SQL Injection (SQLi)</b>	The attacker injects SQL statements that can read or modify database data. In the case of advanced SQL Injection attacks, the attacker can use SQL commands to write arbitrary files to the server and even execute OS commands. This may lead to full system compromise.	<ul style="list-style-type: none"> <li>• Authentication bypass</li> <li>• Information disclosure</li> <li>• Data loss</li> <li>• Sensitive data theft</li> <li>• Loss of data integrity</li> <li>• Denial of service</li> <li>• Full system compromise.</li> </ul>
<b>XPath injection</b>	The attacker injects data into an application to execute crafted XPath queries. They can use them to access unauthorized data and bypass authentication.	<ul style="list-style-type: none"> <li>• Information disclosure</li> <li>• Authentication bypass</li> </ul>

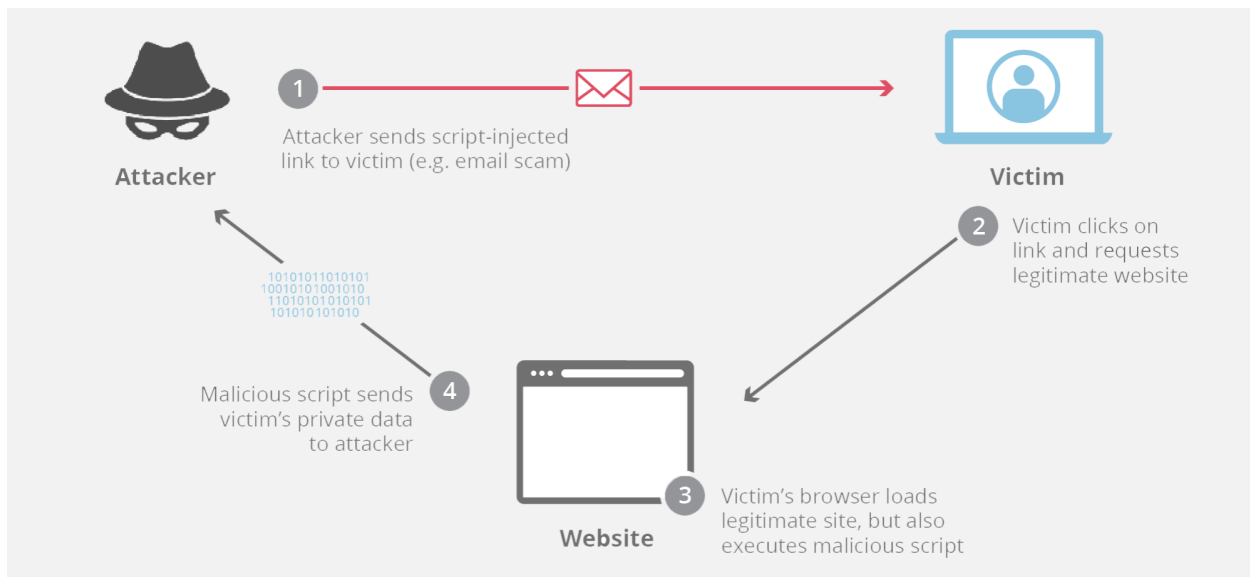


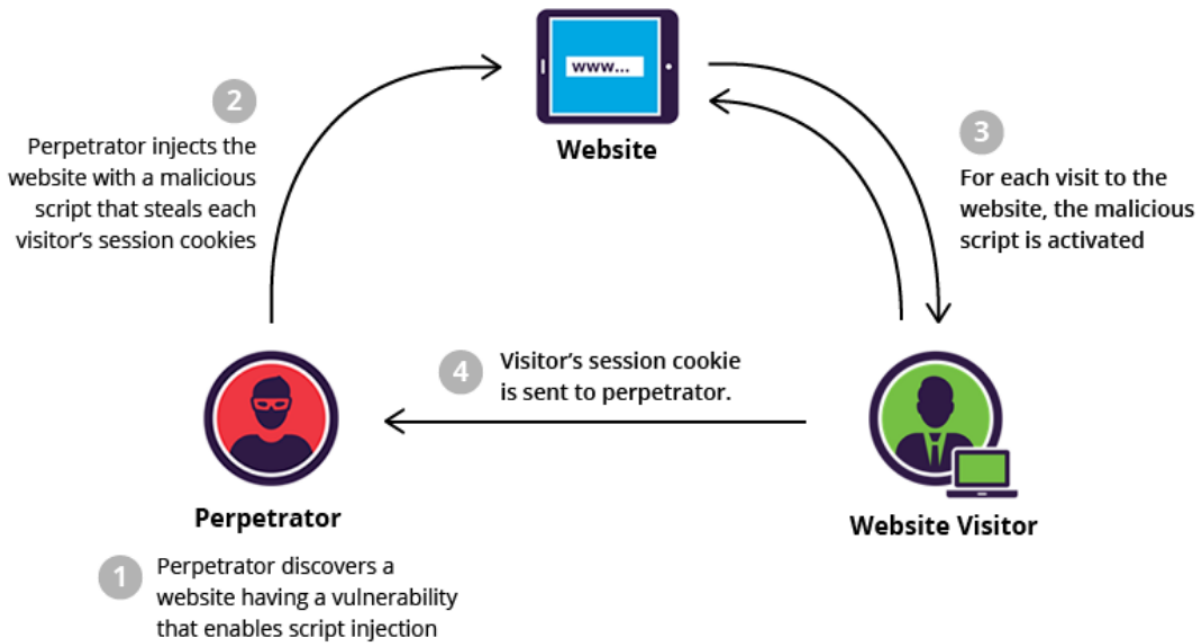
## Cross Site Scripting (XSS)

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users.

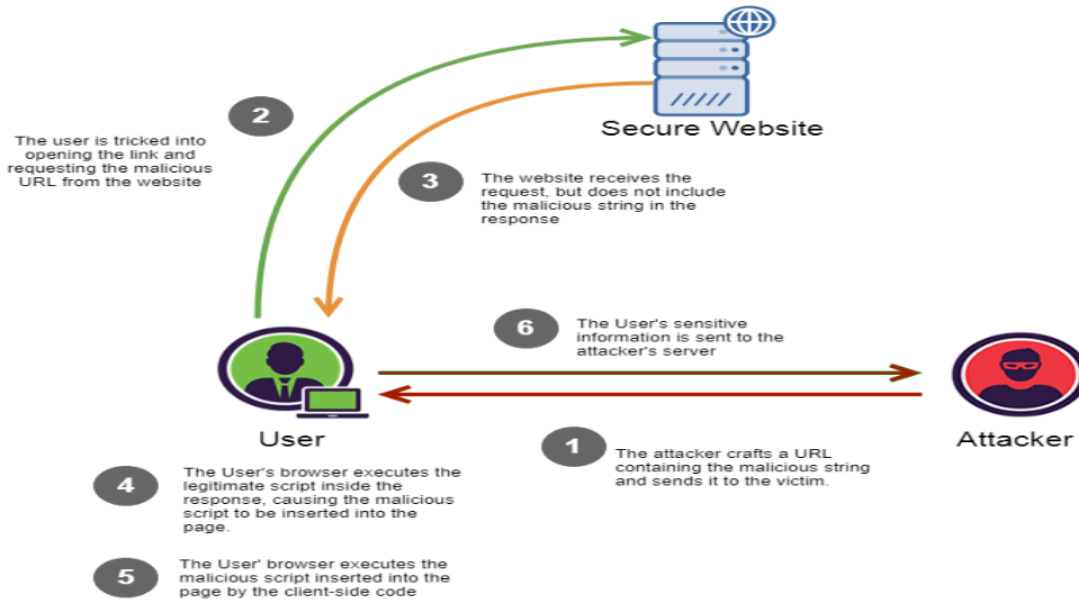
- XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.

- Three types: Reflected XSS,





## Stored XSS



## DOM Based XSS

### TOOLS:

GOOGLE DORKS

BURPSUITE

SCRIPT: `<script>alert(123)</script>`



WEB: <http://brodyaga.ru/pages/search.php>

WEB: <https://www.fontel.com/>

## How to prevent XSS attacks

- Filter/Validating input on arrival.
- Encode data on output.
- Use appropriate response headers
- Content Security Policy.

## Threats

A cyber threat is a potential for violation of cyber security that exists when there is a circumstance, capability, action, or event that could cause a data breach or any other type of unauthorized access.

Any vulnerability that can be exploited is a cyber threat. Cyber threats can come in both intentional and accidental ways:

- **Intentional cyber threat:** An example is a cybercriminal installing the WannaCry ransomware attack, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.
- **WannaCry**

The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, targeting only the Microsoft Windows operating systems.

The initial infection was likely through an exposed vulnerable SMB port, rather than email phishing as initially assumed. However, email phishing was the main method of spreading the WannaCry ransomware.

The WannaCry ransomware attack had exploited a vulnerability in Windows OS called EternalBlue.





### Impact

- This attack impacted a number of businesses, institutions and





hospitals all over the world.

- Businesses like Nissan and Renault had to pause their activities after some of their computers were affected.

- In hospitals, computer systems used for various purposes were affected, like MRI scanners and computers.

- Many critics said that this attack could have been prevented if people took steps, to solve the flaws on which the attacks were based, earlier.

- Some even blame the governments for their inability to secure vulnerabilities.

- Estimates state that around 200,000 to 300,000 computer systems were affected in this attack in approximately 150 countries.

- **Accidental cyber threats:** Poorly configured S3 bucket security leading to a big data breach. Check your Amazon S3 security or someone else will.

This is why understanding the difference between cybersecurity and information security, as well as how to perform a cybersecurity risk assessment is more important than ever. Your organization needs to have a set of policies and procedures to manage your information security in accordance with risk management principles and have countermeasures to protect financial, legal, regulatory, and reputational concerns.

Should a cyber attack lead to a security incident, your organization should have steps to detect, classify, manage, and communicate it to customers where applicable. The first logical step is to develop an incident response plan and eventually a cybersecurity team.

Cyber threats are security incidents or circumstances with the potential to have a negative outcome to your network or other data management systems. Examples of common types of security threats include phishing attacks that result in the installation of malware that infects your data, failure of a staff member to follow data protection protocols that causes a data breach or even a tornado that takes down your company's data headquarters, disrupting access.



When threat probability is multiplied by the potential loss that may result, cybersecurity experts refer to this as risk.

An object, person, or other entity that represents a constant danger to an asset

- Management must be informed of the different threats facing the organization

- By examining each threat category, management effectively protects information through policy, education, training, and technology controls

- 2004 Computer Security Institute (CSI) / Federal Bureau of Investigation (FBI) survey found: – 79% of organizations reported cyber security breaches within the last 12 months – 54% of those orgs. reported financial losses over \$141 million

- A threat is a specific means by which a risk can be realized by an adversary – Context specific (a fact of the environment) – An attack vector is a specific threat (e.g., key logger)

- A threat model is a collection of threats that deemed important for a particular environment – E.g., should be addressed – A set of “security requirements” for a system

- Take the survey with a grain of salt – Underreporting, fear of bad publicity – Cybercrime: easy \$\$ at perceived low risk to attacker

Threats to Info. Security

Threat Category	Examples
Acts of human error or failure	Accidents, employee mistakes
Intellectual property compromise	Piracy, copyright infringement
Deliberate espionage or trespass	Unauthorized access, data collection
Deliberate information extortion	Blackmail of info. Disclosure
Deliberate sabotage or vandalism	Destruction of systems or info.
Deliberate theft	Illegally taking equipment or info.
<b>Deliberate software attacks</b>	<b>Viruses, worms, denial of service</b>
Forces of nature	Fires, floods, earthquakes
Deviations in service from providers	Power and Internet provider issues
Technological hardware failures	Equipment failure



Technological software failures	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

## TYPES OF CYBER SECURITY THREATS

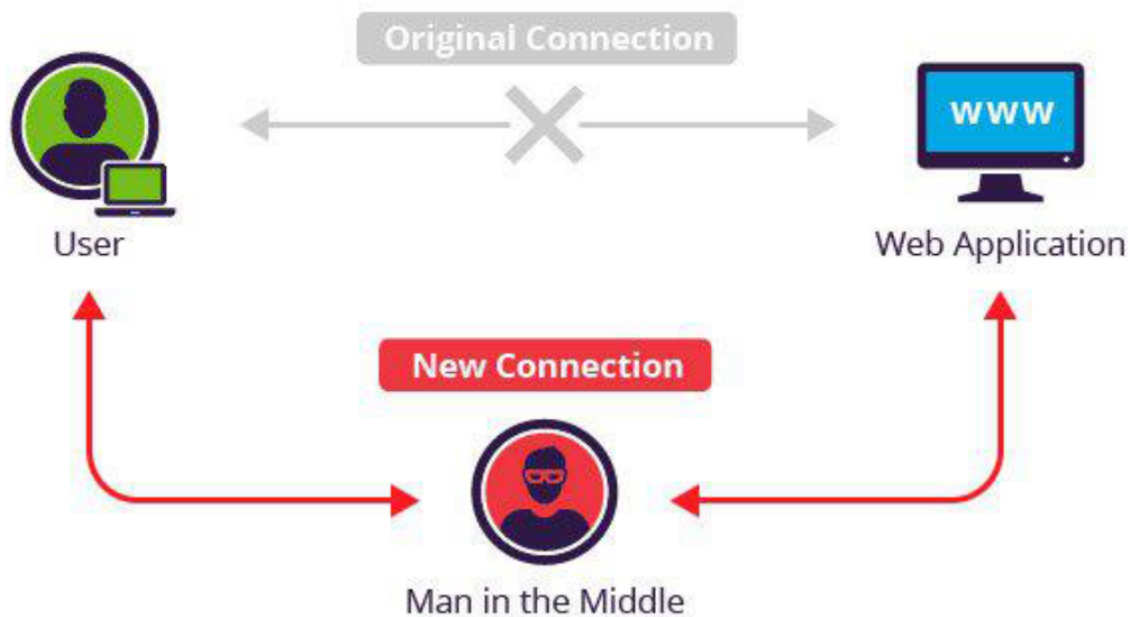
Just as there is a plethora of various germs and diseases that can attack the human body, there are numerous threats that can affect hardware, software and the information you store. Some of the major ones include the following:

- **Viruses:** similar to the way the common cold replicates itself repeatedly in one person's body and is then spread, a software virus is designed in such a way that can be easily transmitted from one computer or system to another. Often sent as email attachments, viruses corrupt and co-opt data, interfere with your security settings, generate spam and may even delete content.
- **Computer worms** are similar; they spread from one computer to the next by sending itself to all of the user's contacts and subsequently to all of the contacts' contacts.
- **Trojans:** these malicious pieces of software insert themselves into a legitimate program. Often, people voluntarily let trojans into their systems in the form of email messages from a person or an advertiser they trust. As soon as the accompanying attachment is open, your system becomes vulnerable to the malware within.
- **Bogus security software** that tricks users into believing that their system has been infected with a virus. The accompanying security software that the threat actor provides to fix the problem actually causes it.
- **Adware** that tracks your browsing habits and causes particular advertisements to pop up. Although this is common and often something you may even agree to, adware is sometimes foisted upon you without your consent. Similarly, spyware is an intrusion that may steal sensitive data such as passwords and credit card numbers from your internal systems.
- **Denial of service (DOS) attack:** this occurs when hackers deluge a website with traffic, making it impossible for users to access its content. A distributed denial of service (DDOS) attack is more forceful and aggressive



since it is initiated from several servers simultaneously. As a result, a DDOS attack is harder to mount defenses against.

- **Phishing attacks** are social engineering infiltrations whose goal is to wrongfully obtain sensitive data such as passwords and credit card numbers. Via emails or links, the hacker causes malware to be downloaded and installed. Many phishing attacks appear to come from trusted companies and financial institutions and ask users to verify their identity, thus leaving them open to hacking.
- **SQL injections** are network threats that involve using malicious code to infiltrate cyber vulnerabilities in data systems. As a result, data can be stolen, changed or destroyed. This type of attack is quickly becoming the most serious network security issue.
- **Man-in-the-middle attacks** involve a third party intercepting and exploiting communications between two entities that should remain private. Not only does eavesdropping occur but also information can be changed or misrepresented by the intruder, causing inaccuracy and even security breaches.



- **Rootkit tools** gain remote access to systems without permission and can lead to the installation of malware and the stealing of passwords and other data.

## Harmful Acts

- Harmful Acts committed form or against a computer or network
- Illegal computer-mediated activities that can be conducted through global electronic networks
- Unlawful acts wherein the computer is either a tool or target or both
- Online or internet-based illegal acts



## **Cyber Criminals:**

Cybercrime involves such activities as child pornography ,credit card fraud, cyber stalking, defaming another online, gaining un authorized access to computer systems, ignoring copyright, software licensing and trade mark protection, overriding encryption to make illegal copies, software piracy and stealing another's identity to perform criminal acts.

They can be categorized into 3 groups.

### **1. Type I: Cybercriminals- hungry for recognition**

- hobby hackers
- IT professionals
- Terrorist organizations

### **2. Type II: Cybercriminals-not interested in recognition**

- psychological perverts
- financially motivated hackers
- organized criminals

### **3. Type III: Cybercriminals- The insiders**

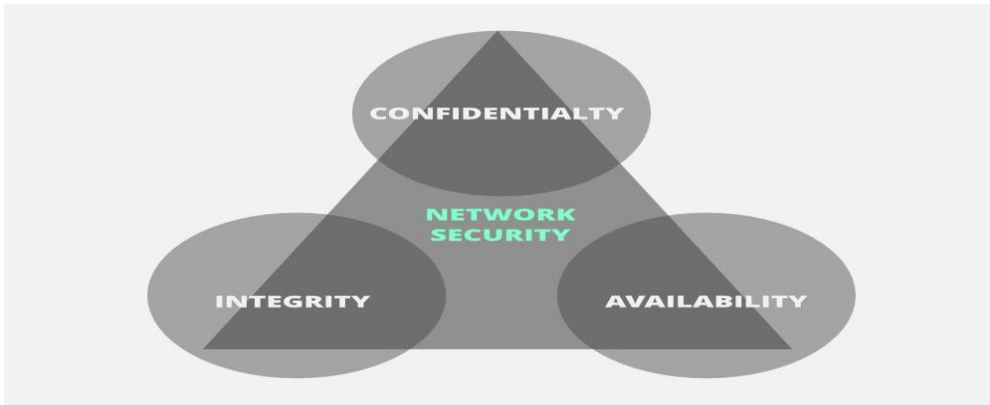
- disgruntled or former employees seeking revenge
- competing companies using employees to gain economic advantage through damage and/or theft.

## **The CIA triad :**

The **CIA** triad is one of the most important model which is designed to guide policies for information security within an organization.

CIA stands for :

1. Confidentiality
2. Integrity
3. Availability

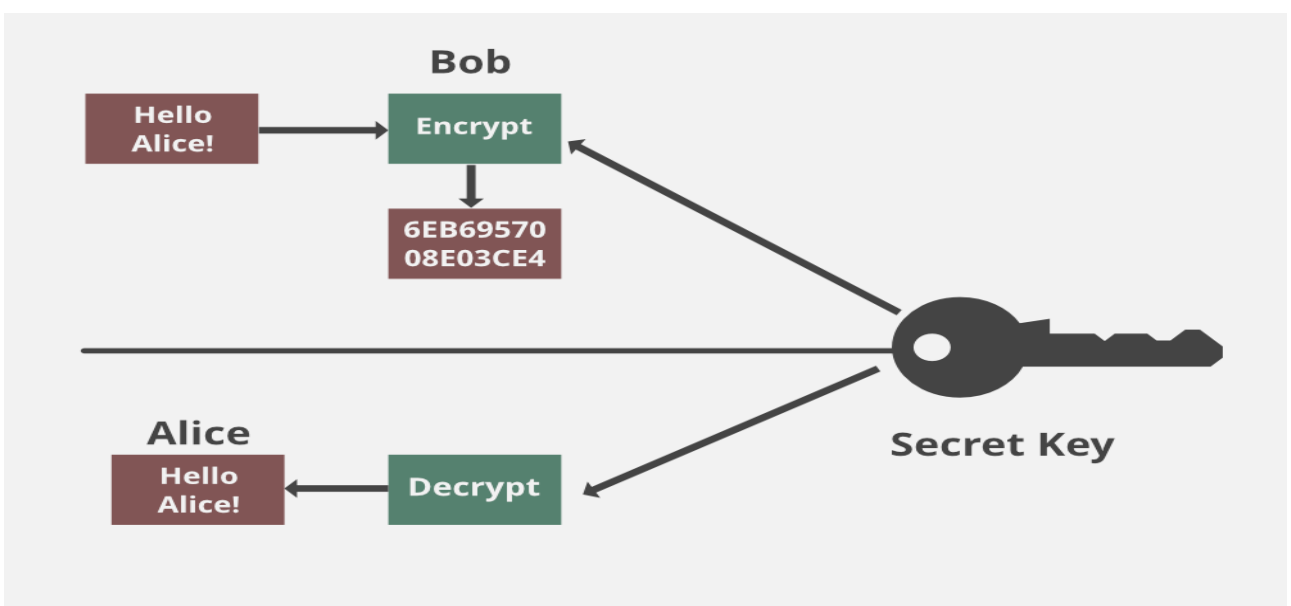


These are the objectives which should be kept in mind while securing a network.

### **Confidentiality:**

Confidentiality means that only the authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to our information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it.

VPN stands for Virtual Private Network and helps the data to move securely over the network.





**Integrity :**

The next thing to talk about is integrity. Well, the idea here is making sure that data has not been modified. Corruption of data is a failure to maintain data integrity.

**Availability :**

This means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over and prevent bottleneck in a network. Attacks such as DoS or DDoS may render a network unavailable as the resources of the network gets exhausted. The impact may be significant to the companies and users who rely on the network as a business tool. Thus, proper measures should be taken to prevent such attacks.

**Motive of attacks:**

The most common types of cyber-crime affecting small businesses are phishing emails, malware attacks and ransom ware, which analysts estimate costs on average £3,000 per business.

**Cash**

A primary motivation for hackers is the money they can obtain by stealing your passwords, bank details, holding your customer information for ransom or selling your data to competitors or on the dark web.

**Challenge**

A large portion of hackers are driven by the opportunity to break the unbreakable system and gaining the recognition from their peers. This competitive behaviour drives groups of hackers to challenge each other to cause disruption at the expense of another business.

**Hacktivism**

Infamous hacker groups use their skills to target large organisations and embarrass their IT teams, break their sophisticated security systems and humiliate the upper management.

**Revenge**

Certain types of hackers are motivated by anger and use their skills to directly affect a person, group or company without any fear of repercussion.

## Subversion

Hackers have been accused of meddling in current and corporate affairs - a modern-day version of espionage.

## Infamy

Hackers are motivated by a sense of achievement, working independently or in groups they want to be recognised. Social media has given them a platform to boast about their exploits on a global scale.

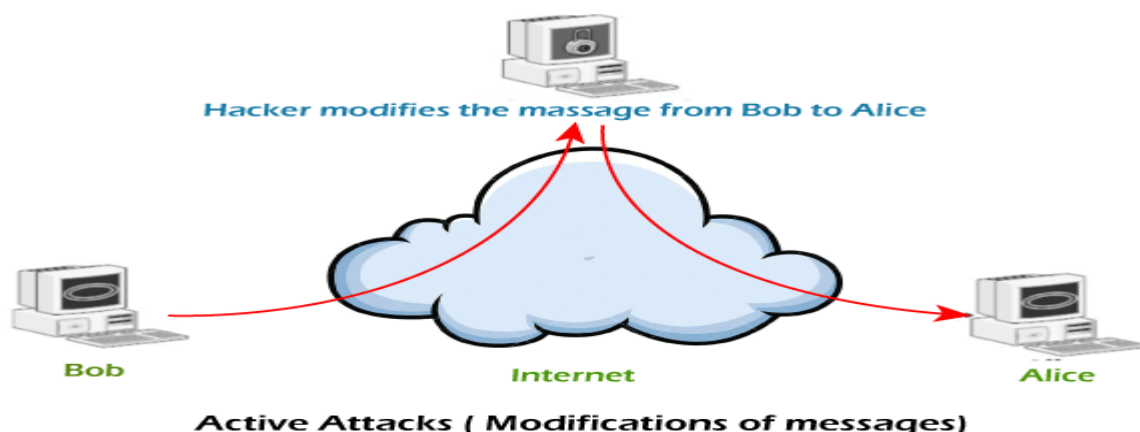
## What is a Security attack?

These are the unauthorized or illegal actions that are taken against the government, corporate, or private IT assets in order to destroy, modify, or steal the sensitive data. They are further classified into active and passive attacks, in which the attacker gets unlawful access to the system's resources.

## Active attacks

In active attacks, the attacker intercepts the connection and efforts to modify the message's content. It is dangerous for integrity and availability of the message. Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service. The system resources can be changed due to active attacks. So, the damage done with active attacks can be harmful to the system and its resources.

In the below image, we can see the process of active attacks.



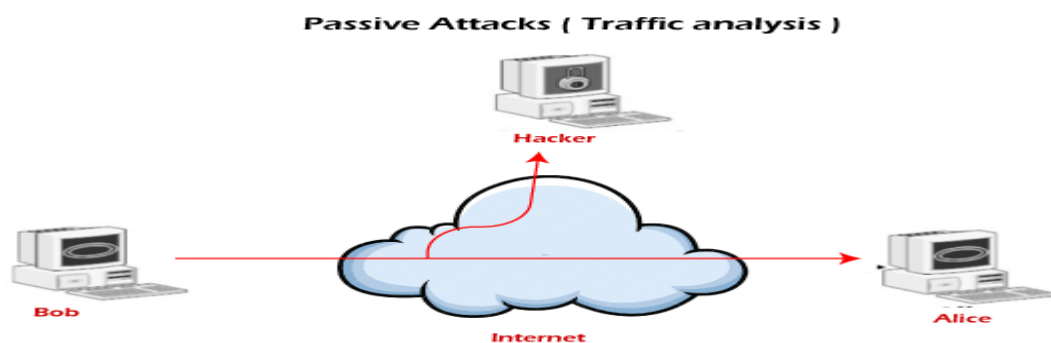
In active attacks, the victim gets notified about the attack. The implication of an active attack is typically difficult and requires more effort. Active attacks can be

prevented by using some techniques. We can try the below-listed measures to prevent these attacks -

- Use of one-time password help in the authentication of the transactions between two parties.
- There could be a generation of the random session key that will be valid for a single transaction. It should prevent the malicious user from retransmitting the actual information once the session ends.

### Passive attacks

In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes. The attacker does not try to change the information or content he/she gathered. Although passive attacks do not harm the system, they can be a danger for the confidentiality of the message.



Unlike active attacks, in passive attacks, victims do not get informed about the attack. It is difficult to detect as there is no alteration in the message. Passive attacks can be prevented by using some encryption techniques. We can try the below-listed measures to prevent these attacks -

- We should avoid posting sensitive information or personal information online. Attackers can use this information to hack your network.
- We should use the encryption method for the messages and make the messages unreadable for any unintended intruder.

### Active attack v/s Passive attack

Now, let's see the comparison chart between Active attack and Passive attack. We are comparing both security attacks on the basis of some characteristics.

<b>On the basis of</b>	<b>Active attack</b>	<b>Passive attack</b>
<b>Definition</b>	In active attacks, the attacker intercepts the connection and efforts to modify the message's content.	In passive attacks, the attacker observes the messages, then copy and save them and can use it for malicious purposes.
<b>Modification</b>	In an active attack, the attacker modifies the actual information.	In passive attacks, information remains unchanged.
<b>Victim</b>	In active attacks, the victim gets notified about the attack.	Unlike active attacks, in passive attacks, victims do not get informed about the attack.
<b>System's impact</b>	The damage done with active attacks can be harmful to the system and its resources.	The passive attacks do not harm the system.
<b>System resources</b>	In active attacks, the system resources can be changed.	In passive attacks, the system resources remain unchanged.
<b>Dangerous for</b>	They are dangerous for the integrity and availability of the message.	They can be dangerous for confidentiality of the message.
<b>Emphasis on</b>	In active attacks, attention is on detection.	In active attacks, attention is on prevention.
<b>Types</b>	Active attacks involve Masquerade, Modification of message, Repudiation, Replay, and Denial of service.	It involves traffic analysis, the release of a message.

<b>Prevention</b>	Active attacks are tough to restrict from entering systems or networks.	Unlike active attacks, passive attacks are easy to prohibit.
-------------------	---	--

### Software attacks:

The software attack surface is **the complete profile of all functions in any code running in a given system that are available to an unauthenticated user**. ... The software attack surface is particularly at risk in the case of Web applications, which expose the coding to the Internet.

Ex: **Malware**, in which malicious software is used to attack information systems. Ransomware, spyware and Trojans are examples of malware.

### Hardware attacks:

It is a **process of protecting hardware against vulnerabilities** that are targeting these devices. It is a process of protecting software against malicious attack and other hacker's risks. ... Hardware cannot modify features just like software.

Hardware attacks are not as well-known as these software attacks, but they are just as dangerous. They **involve directly exploiting interaction with a system's electronic components**. These sneak attacks are particularly effective against connected objects.

Ex: Directory traversal, Bad USB, PCB tampering etc

### IP Spoofing:

Spoofing is a specific type of cyber-attack in which someone attempts to use a computer, device, or network to trick other computer networks by masquerading as a legitimate entity.

### What does IP spoofing do?

IP spoofing enables an attacker to replace a packet header's source IP address with a fake, or spoofed IP address. The attacker does this by intercepting an IP packet and modifying it, before sending it on to its destination. ... As you can see, IP spoofing facilitates anonymity by concealing source identities.

Every packet comprises an IP address header that possesses data about the IP address of the sender and the receiver and other relevant information about the packet under consideration.

### **Cyber Crime:**

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device.

Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.

Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

Rarely, cybercrime aims to damage computers for reasons other than profit. These could be political or personal.

### **Types of cybercrime**

Here are some specific examples of the different types of cybercrime:

Email and internet fraud.

Identity fraud (where personal information is stolen and used).

Theft of financial or card payment data.

Theft and sale of corporate data.

Cyberextortion (demanding money to prevent a threatened attack).

Ransomware attacks (a type of cyberextortion).

Cryptojacking (where hackers mine cryptocurrency using resources they do not own).

Cyberespionage (where hackers access government or company data).

### **Cyber Terrorism:**

Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

What are the methods of cyber terrorism?

Typical practices of cyberterrorists may include: Denial of Service (Dos) attacks and Distributed Denial of Service attacks (DDos) Web defacement which may include negative or derogatory comments against the government, political parties or other religious organizations. Misinformation campaigns.

### **Cyber Espionage:**

Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

There are 2 types of espionage.

The first of which defines the two types of espionage: covert operations and covert intelligence, distinguishing between the human and cyber variants of both.

### **Cyber Threats:**

A cyber or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber-attacks include threats like computer viruses, data breaches, and Denial of Service (DoS) attacks.

Top 10 Computer Security Threats to Prepare for in 2021.

- Phishing Attacks. ...
- Cloud Jacking. ...
- Network Perimeter and Endpoint Security. ...
- Mobile Malware. ...
- 5G-to-Wi-Fi Security Vulnerabilities. ...
- Internet of Things (IoT) Devices. ...
- Deepfakes. ...
- Highly Developed Ransomware Attacks.

### **Cyber Warfare:**

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

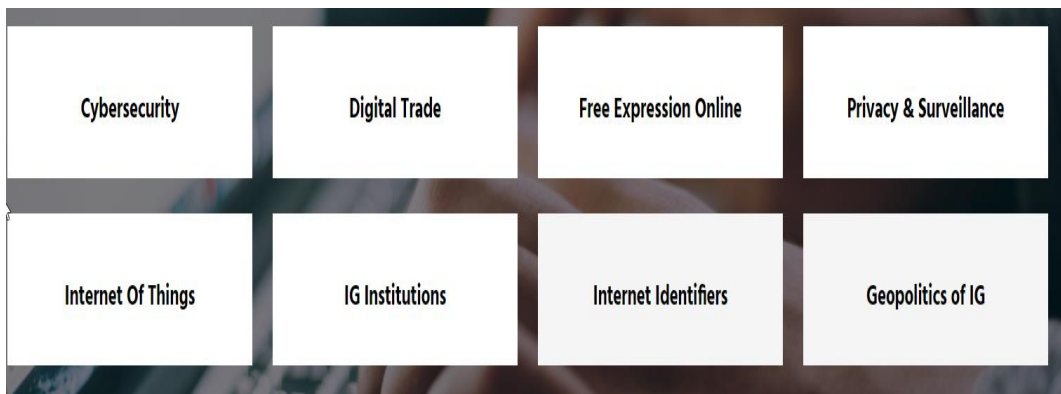
### **Internet governance**

Internet governance refers to the rules, policies, standards and practices that coordinate and shape global cyberspace.



The Internet is a vast network of independently-managed networks, woven together by globally standardized data communication protocols (primarily, Internet Protocol, TCP, UDP & DNS ). The common adoption and use of these protocols unified the world of information and communications like never before. Millions of digital devices and massive amounts of data, software applications, and electronic services became compatible and interoperable. The Internet created a new environment, a complex and dynamic “cyberspace.”

The term “Internet governance” first started to be used in connection with the governance of Internet identifiers such as domain names and IP addresses, which led to the formation of ICANN. Since then, the economic, political, social and military implications of Internet governance have expanded to embrace a number of other areas of policy:



The Internet impacts global interests and its governance "includes more than Internet names and addresses, issues dealt with by the Internet Corporation for Assigned Names and Numbers (ICANN); it also includes other significant public policy issues, such as critical Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet". For these reasons, a single entity cannot and has not been designated as an international governance body. Instead, the Internet is primarily governed internationally by multiple stakeholders - government, the private sector, academia, and civil society - covering a range of technical and non-technical issues. Nevertheless, countries vary in terms of their views on which stakeholders should play a primary role in Internet governance. While some countries believe that multiple stakeholders should be responsible for Internet governance, other countries believe that Internet governance should be the exclusive domain of the state.

## Methods of Defense

We investigate the legal and ethical restrictions on computer-based crime. But unfortunately, computer crime is certain to continue for the foreseeable future. For this reason, we must look carefully at controls for preserving confidentiality, integrity, and availability. Sometimes these controls can prevent or mitigate attacks; other, less powerful methods can only inform us that security has been compromised, by detecting a breach as it happens or after it occurs.

Harm occurs when a threat is realized against vulnerability. To protect against harm, then, we can neutralize the threat, close the vulnerability, or both. The possibility for harm to occur is called **risk**. We can deal with harm in several ways. We can seek to

- *prevent it*, by blocking the attack or closing the vulnerability
- *deter it*, by making the attack harder but not impossible
- *deflect it*, by making another target more attractive (or this one less so)
- *detect it*, either as it happens or sometime after the fact
- *recover* from its effects

Of course, more than one of these can be done at once. So, for example, we might try to prevent intrusions. But in case we do not prevent them all, we might install a detection device to warn of an imminent attack. And we should have in place incident response procedures to help in the recovery in case an intrusion does succeed.

## Controls

To consider the controls or countermeasures that attempt to prevent exploiting a computing system's vulnerabilities, we begin by thinking about traditional ways to enhance physical security. In the Middle Ages, castles and fortresses were built to protect the people and valuable property inside. The fortress might have had one or more security characteristics, including

- a strong gate or door, to repel invaders
- heavy walls to withstand objects thrown or projected against them
- a surrounding moat, to control access
- arrow slits, to let archers shoot at approaching enemies
- crenellations to allow inhabitants to lean out from the roof and pour hot or vile liquids on attackers
- a drawbridge to limit access to authorized people
- gatekeepers to verify that only authorized people and goods could enter

Similarly, today we use a multipronged approach to protect our homes and offices. We may combine strong locks on the doors with a burglar alarm, reinforced windows, and even a nosy neighbor to keep an eye on our valuables. In each case, we select one or more ways to deter an intruder or attacker, and we base our selection not only on the value of what we protect but also on the effort we think an attacker or intruder will expend to get inside.

Computer security has the same characteristics. We have many controls at our disposal. Some are easier than others to use or implement. Some are cheaper than others to use or implement. And some are more difficult than others for intruders to override. We use one or more controls, according to what we are protecting, how the cost of protection compares with the risk of loss, and how hard we think intruders will work to get what they want.

**Encryption** is the formal name for the scrambling process. We take data in their normal, unscrambled state, called **cleartext**, and transform them so that they are unintelligible to the outside observer; the transformed data are called **enciphered text** or **ciphertext**. Using encryption, security professionals can virtually nullify the value of an interception and the possibility of effective modification or fabrication. In Chapters 2 and 12 we study many ways of devising and applying these transformations.

Encryption clearly addresses the need for confidentiality of data. Additionally, it can be used to ensure integrity; data that cannot be read generally cannot easily be changed in a meaningful manner. Furthermore, as we see throughout this book, encryption is the basis of **protocols** that enable us to provide security while accomplishing an important system or network task. A protocol is an agreed-on sequence of actions that leads to a desired result. For example, some operating system protocols ensure availability of resources as different tasks and users request them. Thus, encryption can also be thought of as supporting availability. That is, encryption is at the heart of methods for ensuring all aspects of computer security.

Although encryption is an important tool in any computer security tool kit, we should not overrate its importance. Encryption does not solve all computer security problems, and other tools must complement its use. Furthermore, if encryption is not used properly, it may have no effect on security or could even degrade the performance of the entire system. Weak encryption can actually be worse than no encryption at all, because it gives users an unwarranted sense of

protection. Therefore, we must understand those situations in which encryption is most useful as well as ways to use it effectively.

## Software Controls

If encryption is the primary way of protecting valuables, programs themselves are the second facet of computer security. Programs must be secure enough to prevent outside attack. They must also be developed and maintained so that we can be confident of the programs' dependability.

Program controls include the following:

- *internal program controls*: parts of the program that enforce security restrictions, such as access limitations in a database management program
- *operating system and network system controls*: limitations enforced by the operating system or network to protect each user from all other users
- *independent control programs*: application programs, such as password checkers, intrusion detection utilities, or virus scanners, that protect against certain types of vulnerabilities
- *development controls*: quality standards under which a program is designed, coded, tested, and maintained to prevent software faults from becoming exploitable vulnerabilities

We can implement software controls by using tools and techniques such as hardware components, encryption, or information gathering. Software controls frequently affect users directly, such as when the user is interrupted and asked for a password before being given access to a program or data. For this reason, we often think of software controls when we think of how systems have been made secure in the past. Because they influence the way users interact with a computing system, software controls must be carefully designed.

## Hardware Controls

Numerous hardware devices have been created to assist in providing computer security. These devices include a variety of means, such as

- hardware or smart card implementations of encryption
- locks or cables limiting access or deterring theft
- devices to verify users' identities
- firewalls
- intrusion detection systems
- circuit boards that control access to storage media

## **Policies and Procedures**

Sometimes, we can rely on agreed-on procedures or policies among users rather than enforcing security through hardware or software means. In fact, some of the simplest controls, such as frequent changes of passwords, can be achieved at essentially no cost but with tremendous effect. Training and administration follow immediately after establishment of policies, to reinforce the importance of security *policy* and to ensure their proper use.

We must not forget the value of community standards and expectations when we consider how to enforce security. There are many acts that most thoughtful people would consider harmful, and we can leverage this commonality of belief in our policies. For this reason, legal and ethical controls are an important part of computer security. However, the law is slow to evolve, and the technology involving computers has emerged relatively suddenly. Although legal protection is necessary and desirable, it may not be as dependable in this area as it would be when applied to more well-understood and long-standing crimes.

Society in general and the computing community in particular have not adopted formal standards of ethical behavior. As we see in Chapter 11, some organizations have devised codes of ethics for computer professionals. However, before codes of ethics can become widely accepted and effective, the computing community and the general public must discuss and make clear what kinds of behavior are inappropriate and why.

## **Physical Controls**

Some of the easiest, most effective, and least expensive controls are *physical controls*. Physical controls include locks on doors, guards at entry points, backup copies of important software and data, and physical site planning that reduces the risk of natural disasters. Often the simple physical controls are overlooked while we seek more sophisticated approaches.

## **Cyber Risk management**

Cyber threats are constantly evolving. The most effective way to protect your organisation against cyber attacks is to adopt a risk-based approach to cyber security, where you regularly review your risks and whether your current measures are appropriate.

IT Governance can help you develop a cyber threat management strategy, enabling you to take a systematic approach to managing your security challenges.

### **Cyber risk management:**

Cyber risk management is the process of identifying, analysing, evaluating and addressing your organisation's cyber security threats.

The first part of any cyber risk management programme is a cyber risk assessment. This will give you a snapshot of the threats that might compromise your organisation's cyber security and how severe they are.

Based on your organisation's risk appetite, your cyber risk management programme then determines how to prioritise and respond to those risks.

### **The cyber risk management process**

Although specific methodologies vary, a risk management programme typically follows these steps:

1. Identify the risks that might compromise your cyber security. This usually involves identifying cyber security vulnerabilities in your system and the threats that might exploit them.
2. Analyse the severity of each risk by assessing how likely it is to occur, and how significant the impact might be if it does.
3. Evaluate how each risk fits within your risk appetite (your predetermined level of acceptable risk).
4. Prioritise the risks.
5. Decide how to respond to each risk. There are generally four options:
  - Treat – modify the likelihood and/or impact of the risk, typically by implementing security controls.
  - Tolerate – make an active decision to retain the risk (e.g. because it falls within the established risk acceptance criteria).
  - Terminate – avoid the risk entirely by ending or completely changing the activity causing the risk.
  - Transfer – share the risk with another party, usually by outsourcing or taking out insurance.
6. Since cyber risk management is a continual process, monitor your risks to make sure they are still acceptable, review your controls to make sure they are still fit for purpose, and make changes as required. Remember that your risks are continually changing as the cyber threat landscape evolves, and your systems and activities change.

Standards and frameworks that mandate a cyber risk management approach

### **ISO 27001**

ISO/IEC 27001:2013 – the international standard for information security management. Clause 6.1.2 of ISO 27001 states that an information security risk assessment must:

- Establish and maintain information security risk criteria;
- Ensure that repeated risk assessments produce “consistent, valid and comparable results”;
- “identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system”;
- Identify the owners of those risks; and
- Analyse and evaluate information security risks according to the criteria established earlier.

### **The NCSC’s 10 steps to cyber security**

The NCSC’s (National Cyber Security Centre) 10 steps to cyber security - a set of ten practical steps that organisations can take to improve the security of their networks and the information carried on them. Defining and communicating your board’s information risk management regime is central to your organisation’s overall cyber security strategy and the first of the ten steps.

### **The CIS Controls**

CIS (Center for Internet Security) Controls - the CIS Controls, formerly the 20 Critical Controls for Effective Cyber Defense, are a set of 20 actions, also known as CSC (critical security controls), for cyber defence, which provide specific and actionable ways to stop today’s most pervasive and dangerous attacks.

### **The PCI DSS**

The PCI DSS (Payment Card Industry Data Security Standard) - applies to organisations of any size that accept card payments. Protecting digital cardholder data requires adherence to all the PCI DSS data security requirements. There are 12 PCI DSS requirements, which apply to “all system components included in or connected to the cardholder data environment”. Requirements 5 and 6 deal with implementing and maintaining a vulnerability management programme – an essential part of risk management.

## Security Models:

### NIST Cyber Security Framework

National Institute of Standards and Technology (NIST) is a cybersecurity model commonly used by organizations in the US. Establishing and communicating your organization's tolerance for risk is key to increase program maturity, in accordance to this model. The NIST framework also accounts for the rapidly changing nature of cybersecurity threats, and advises its followers to continuously adjust their monitoring techniques and remediation strategies to match the ongoing threat environment.

The NIST cybersecurity model follows **five key phases** to reaching a mature security management program:

1. **Identify** - In the first phase, organizations establish a business-wide approach to cybersecurity management, including an understanding of the current risks to the network, what sensitive information lives throughout the organization, and what critical business operations exist that need to be protected from cybersecurity threats
2. **Protect** - The next step in building program maturity according to NIST's cybersecurity model is to organize and define the defenses necessary to protect the identified critical pieces of your security program.
3. **Detect** - This phase is probably what most organizations dive right into when it comes to cybersecurity program management, including establishing the most effective and encompassing monitoring tools to identify risks efficiently and effectively.
4. **Respond** - The fourth step to increase program maturity according to NIST's cybersecurity model is to tackle the threats to your organization. This is more than just patching your network, but means proper containment of the impact of malicious activity.
5. **Recover** - Just as detection and remediation are important to program maturity, having it in your management process to schedule time to recover and reflect on damages will allow for real program improvements and better protection of your network in the future.

The NIST cybersecurity model acknowledges the current practices most organizations use to protect their network. Instead of starting new, it guides organizations to better use what they're already doing and add in the right steps to reach program maturity.



## ISO 27000

ISO 27000 is an international standard, created by the International Organization for Standardization (ISO) to highlight best practices for information security management systems. This cybersecurity model is more popular among organizations in the European Union, and focuses attention on the three main areas of a mature cybersecurity management program: people, processes, and technology. The recommendations of the ISO 27000 cybersecurity model is broken down into the following areas for security managers to use best practices to reach program maturity:

- Security risk assessment
- Security policy
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management

Similarly to the NIST framework, ISO 27000 guides organizations beyond the typical cyber security management practices to include greater security standards and protections. ISO 27000 includes management of critical physical and operational security measures, and is broken down into ISO 27000 Series to get more specific into the actual implementation and design of this cyber security model.

ISO 27000 Series	
ISO27001	ISMS Requirements
ISO27002	ISMS controls
ISO27003	ISMS implementation guidelines
ISO27004	ISMS Measurements
ISO27005	Risk management
ISO27006	Guidelines for ISO 27000 accreditation bodies

## CIS 20

The final cyber security model many organizations follow to reach program maturity is the CIS 20. Designed by the center for Internet Security after the US defense industry experienced a data breach in 2008, the CIS 20 is a series of 20

controls deemed critical to protect an organization's network from expansive cyber attacks.

The CIS 20 is broken down into 3 main categories of controls:

1. Basic Controls (like inventory control, continuous vulnerability management, and controlled employee privileges)
2. Foundational Controls (like malware defenses, data protection, or wireless access controls)
3. Organizational Controls (like training programs and creation of incident response teams)

The CIS 20 cyber security model is designed to be all-encompassing, and require extreme attention and care to an organization's cyber security management process.

There are many cyber security models for organizations to both choose from, or to be required to follow. It's also important for a lot of businesses to become certified for following a specific framework to best represent themselves compared to their competition.

### **Comprehensive IT Security Policy:**

A comprehensive IT security policy is essentially a battle plan that guides our organization, ensuring that your data and network is guarded from potential security threats. Think of it as a link between your people, processes, and technology.

### **Goals of a comprehensive security policy:**

The CIA Triad refers to the 3 goals of cyber security Confidentiality, Integrity, and Availability of the organizations systems, network and data.

Confidentiality – Keeping sensitive information private. Encryption services can protect your data at rest or in transit and prevent unauthorized access to protected data.

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information. It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when

they will occur. A security policy also considered being a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

### **Need of Security policies-**

#### **1) It increases efficiency.**

The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources. The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

#### **2) It upholds discipline and accountability**

When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law. The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.

#### **3) It can make or break a business deal**

It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information. It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.

# Cyberspace

- Cyberspace can be defined as an intricate environment that involves interactions between people, software, and services.
- It is maintained by the worldwide distribution of information and communication technology devices and networks.
- With the benefits carried by the technological advancements, the cyberspace today has become a common pool used by citizens, businesses, critical information infrastructure, military and governments in a fashion that makes it hard to induce clear boundaries among these different groups.
- The cyberspace is anticipated to become even more complex in the upcoming years, with the increase in networks and devices connected to it.

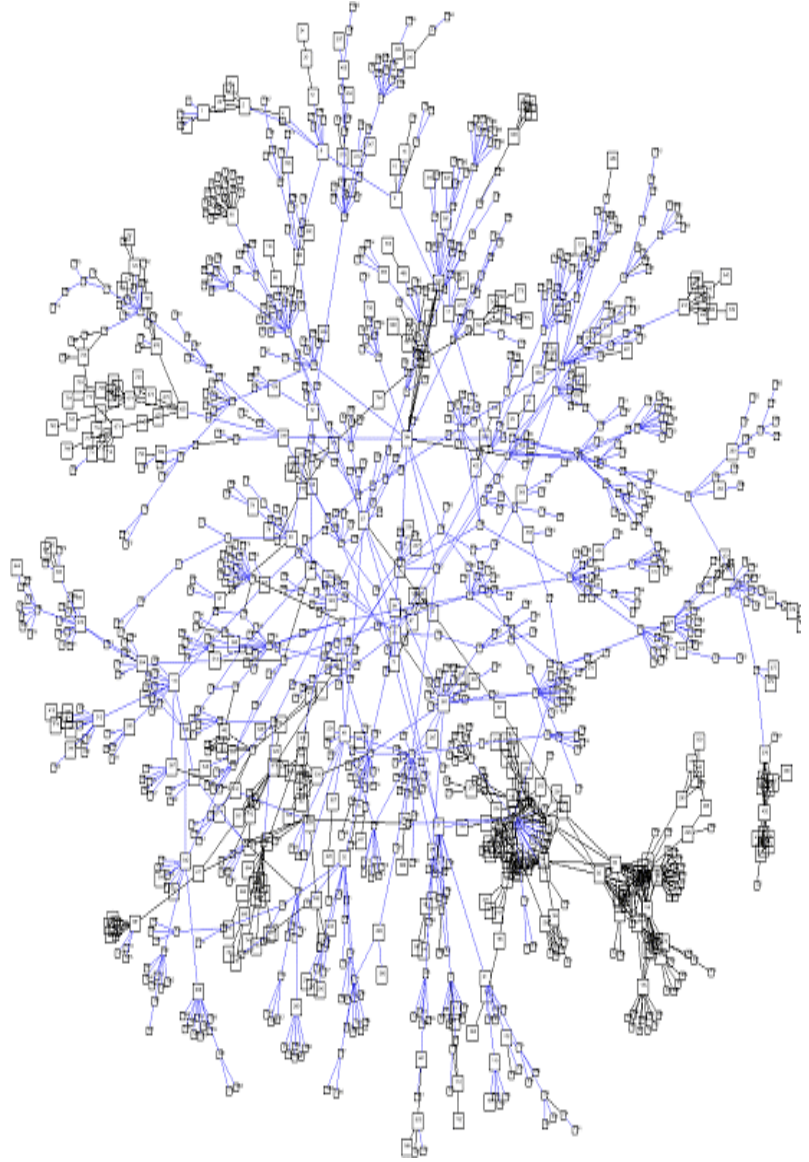
# Concept of Cyberspace

## Cyberspace

Cyberspace is "the environment in which communication over computer networks occurs."

**And almost everybody in one way or the other is connected to it**

**Cyber space includes computers, networks, software's, data storage devices (*such as hard disks, USB disks etc*), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.**



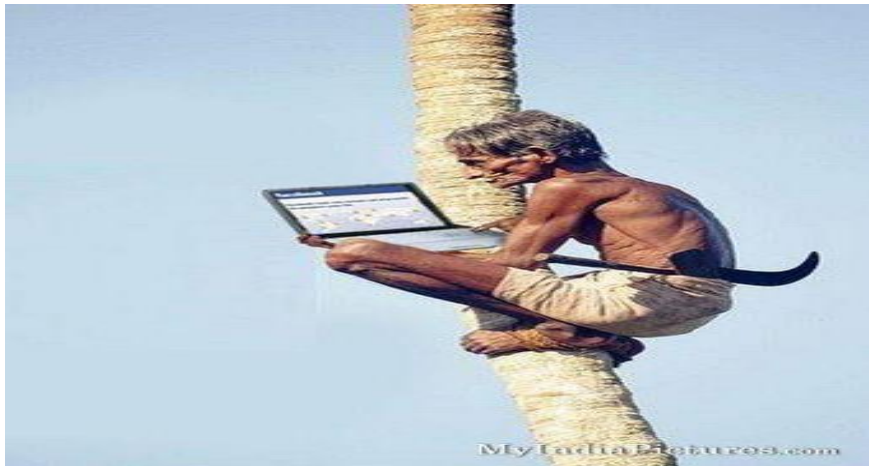
# Concept of Cyberspace



Shepherds are connected to locate their cattle



Hunters are connected to it to locate their prey



Our friend, the farmer is connected to it and "Facebooking" in the coconut tree



Our friends in the remote areas are also connected to it



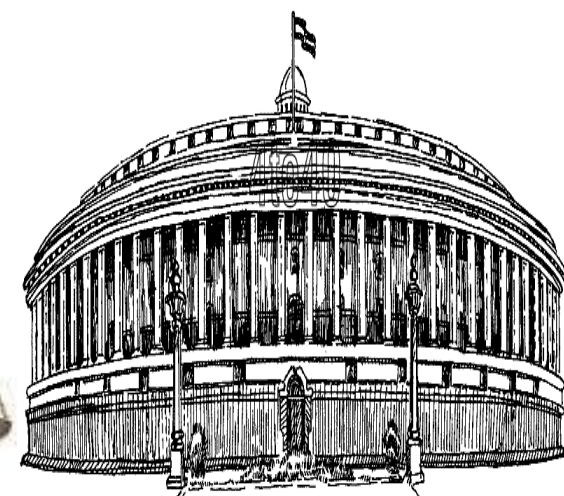
# Concept of Cyberspace



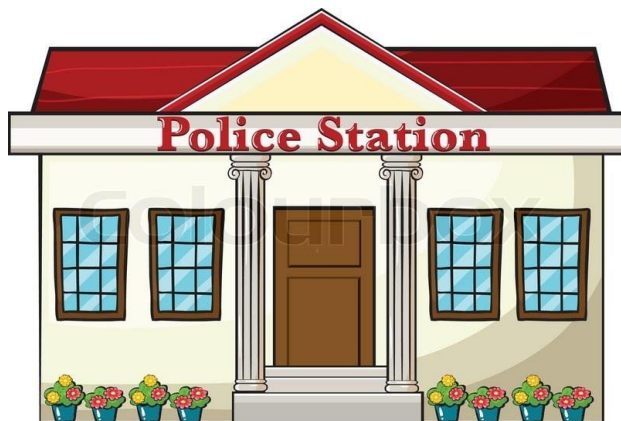
**Government**



**Judiciary**



**Law makers**

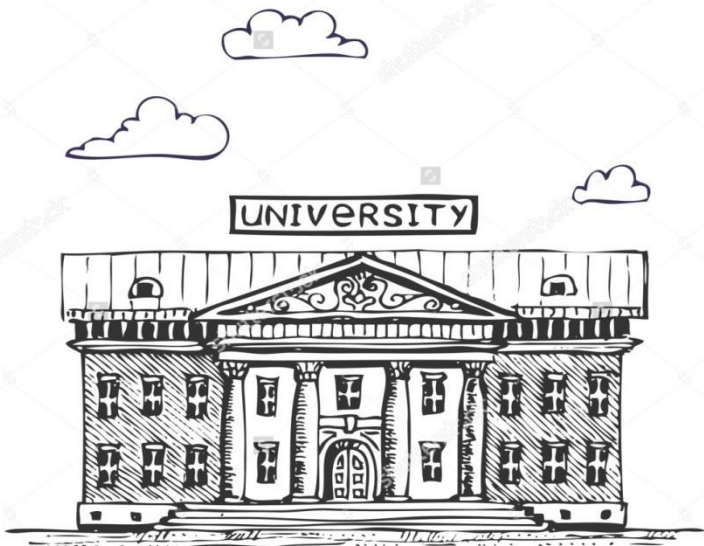




**Transportation Sectors**



**Health Sectors**





- Cyberspace is the dynamic and virtual space
- In 1984, William Gibson published his science fiction book – *Necromancer*, which describes an online world of computers and elements of the society who use these computers. The word cyberspace first appeared in this book. In the book, a hacker of databases stole data for a fee. The author portrayed cyberspace as a three-dimensional virtual landscape. Also, a network of computers creates this space.
- According to him, cyberspace looked like a physical space but was actually a computer generated construction.
- It simply represents the interconnected space between computers, systems, and other networks.
- It exists in the form of bits and bytes – zeroes and ones (0's and 1's). In fact, the entire cyberspace is a dynamic environment of 0's and 1's which changes every second. These are simply electronic impulses. Also, it is an imaginary location where the words of two parties meet in conversation.

- **Cyberspace vs. Physical World**

- Firstly, cyberspace is a digital medium and not a physical space. It is an interactive world and is not a copy of the physical world. Here are some differences between cyberspace and the physical world:

- **Physical World**

Static, well-defined, and incremental

Has fixed contours

- **Cyberspace**

Dynamic, undefined, and exponential

Is as vast as the human imagination and has no fixed shape

- In a human brain, there are countless neurons which create a spectre of life. Similarly, the cyberspace represents millions of computers creating a spectre of digital life. Therefore, cyberspace is a natural extension of the physical world into an infinite world.

# Cyber Law ?

- **Cyber Law is the law governing cyber space.**
- Cyber Law is a generic term referring to all the legal and regulatory aspects of the internet. Everything concerned with or related to or emanating from any legal aspects or concerning any activities of the citizens in the cyberspace comes within the ambit of cyber laws.

# Cyber Law Deals with

- **Cyber Crimes**
- **Electronic or Digital Signatures**
- **Intellectual Property**
- **Data Protection and Privacy**

# Need of Cyber Law

**"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".**

*National Research Council, U S A "Computers at Risk".1991*

# Need of Cyber Law

- **Internet has dramatically changed the way we think, the way we govern, the way we do commerce and the way we perceive ourselves.**
- **Information technology is encompassing all walks of life all over the world.**
- **Cyber space creates moral, civil and criminal wrongs. It has now given a new way to express criminal tendencies.**

# Need of Cyber Law

- **Cyberspace is open to participation by all**
- **“IT” has brought Transition from paper to paperless world**
- **The laws of real world cannot be interpreted in the light of emerging cyberspace to include all aspects relating to different activities in cyberspace**
- **Internet requires an enabling and supportive legal infrastructure in tune with the times**

# The India Cyber Space - IT Act-2000

- **The Information Technology Act, 2000 (IT Act), came into force on *17 October 2000*.**
- **The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.**
- **Information Technology Act 2000 consisted of *94 sections segregated into 13 chapters*.**



# IT Act-2000 : Objectives

- To provide legal recognition for transactions
- To facilitate electronic filing of documents with the Government agencies.
- To amend the *Indian Penal Code, The Indian Evidence Act, 1872, The Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934.*
- Aims to provide the legal framework to all electronic records.

# IT Act-2000

## Snapshot of Important Cyber Law Provisions in India

<i>Offence</i>	<i>Section under IT Act</i>
<b>Tampering with Computer source documents (with out the permission of in charge)</b>	<b>Sec.43</b>
<b>Hacking with Computer systems, Data alteration</b>	<b>Sec.66</b>
<b>Publishing obscene information</b>	<b>Sec.67</b>
<b>Un-authorized access to protected system</b>	<b>Sec.70</b>
<b>Breach of Confidentiality and Privacy</b>	<b>Sec.72</b>
<b>Publishing false digital signature certificates</b>	<b>Sec.73</b>

# IT Act-2000

## Crimes under Indian Penal Code and Special Laws

### *Offence*

### *Sections*

**Sending threatening & Defamatory messages by email**

**Sec 503 & 499 IPC**

**Forgery of electronic records**

**Sec 463 IPC**

**Bogus websites, cyber frauds**

**Sec 420 IPC**

**Email spoofing & Abuse**

**Sec 463 & 500 IPC**

**Web-Jacking**

**Sec 383 IPC**

**Online sale of Drugs**

**NDPS Act**

**Online sale of Arms**

**Arms Act**

# Section 43

**If any person uses a computer or system network without permission of the owner or any other person who is incharge &**

- **Access, download, Copy any data from such computer**
- **Introduces Computer Virus into any computer.**
- **Damages any computer network or computer.**
- **Changes Account Settings.**

## **Punishment**

**He shall be liable to pay damages by the way of compensation not exceeding *1 Crore* to affected person.**

# Section 66

## **Hacking with Computer System**

➤ **Information residing in a computer resources must be either:**

- **Destroyed**
- **Deleted**
- **Altered**
- **Diminished in value or utility**
- **Affected Injuriously**

## **Punishment**

**3 yrs. Or Fine up to 2 lakh.**

# Section 67

- **Publication or transmitted in the electronic form any material which contains sexually explicit acts or conduct.**

## **Punishment**

- **1st conviction with *2 to 5 years* of imprisonment and fine of *1 lakh rupees*.**
- **2nd or subsequent conviction with the imprisonment up to *7-10 years* and also with fine which may extend to *10 lakh rupees*.**

# Some other Sections

- **Section 65 : Tampering with computer source document.**

## **Punishments**

**Offences are punishable with imprisonment up to 3 yrs.  
And/or fine up to Rs. 2 lakh.**

- **Section 69: Interception, monitoring of any information regarding the integrity, Security or defense of India, friendly relations with foreign countries.**

## **Punishment**

**2 lakh and /or jail not extending 5 yrs**

# Some other Sections

- **Section 502A: Publishing, Transmitting images of the private area of a person without his or her consent.**  
**Punishment : 2yrs./2 lakh.**
- **Section 419A: Cheating by any communication device or computer resource**  
**Punishment : 5yrs.**
- **Section 417A: Identity Theft**  
**Punishment: 2yrs.**
- **Section 72: Violation of the privacy policy**  
**Punishment: Fine up to 5 lakh jail not extending 2 yrs.**



# IT Act Amendment-2008

- **The Information Technology Amendment Act, 2008 (IT Act 2008) has been passed by the parliament on *23rd December 2008.***
- **It received the assent of President of India on *5th February, 2009.***
- **The IT Act 2008 has been notified on *October 27, 2009.***

# IT Act Amendment-2008

- **ITA-2008, is a new version of IT Act 2000.**
- **Provides additional focus on Information Security.**
- **Added several new sections on offences including *Cyber Terrorism* and *Data Protection*.**
- **124 sections and 14 chapters.**
- **Schedule I and II have been replaced & Schedules III and IV are deleted.**

# Salient features

- *Digital signature* has been replaced with *Electronic signature*.
- Section 67 of the old Act is amended.
- Sections 66A to 66F prescribe punishment for obscene electronic message transmissions & cyber terrorism.

# Salient features

- **Amended section 69 gives power to the state.**
- **Sections 69 A and B, grant power to the state to direct blocking for public access of any information through any computer resource.**

# SOPA & PIPA

**United States America have many rules to regulate internet content, Currently He is working on :**

- **SOPA (Stop Online Piracy) is a United States bill to expand the ability to fight online trafficking in copyrighted intellectual property.**
- **PIPA (Protect IP Act) is a proposed law of U.S. government.**

# World & Cyber laws

- **The Great firewall of China monitors every movement in cyber space and protect to publish any offensive content.**
- ***China* have a hold on every content which is harmful of dangerous for the government of China.**
- ***Brazil* is considered world's biggest airport for Hackers.**
- ***Iran* is also a dangerous country for the Netizens. He also have a Crime Police unit for crime in Cyber Space.**

# Importance of Cyber Law

- **We are living in highly digitalized world.**
- **All companies depend upon their computer networks and keep their valuable data in electronic form.**
- **Government forms including income tax returns, company law forms etc are now filled in electronic form.**
- **Consumers are increasingly using credit cards for shopping.**

# Importance of Cyber Law

- **Most people are using email, cell phones and SMS messages for communication.**
- **Even in "non-cyber crime" cases, important evidence is found in computers /cell phones e.g. in cases of divorce, murder, kidnapping, organized crime, terrorist operations, counterfeit currency etc.**
- **Since it touches all the aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace therefore Cyber Law is extremely important.**



# Cyber Security: International regulations

# Importance of Legal Framework

- Law takes the principle of territoriality as point of departure;
- Cyber security tools and targets are physical-boundary-independent;
- Agreements between nations create a general common basis for cyber security measures

# Cyber Security Legal Framework

- International Agreements
- EU Legal Framework
- Bilateral Agreements
- National law
- Internal regulations

# Development of International Law

Cyber Security is a rather new area for law\*.

Over the years, the international co-operation on cybercrime has been very active and comprehensive.

The international level of consensus on criminal law has, however, not been achieved.

# International Activities / UN

## General Assembly Resolutions on:

- ① Developments in the Field of Information and Telecommunications in the Context of International Security
- ② Combating the Criminal Misuse of Information Technology
- ③ Creation of a Global Culture of Cybersecurity
- ④ Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures.

# **Other International Activities**

**ITU - Global Cyber security Agenda (GCA)**

**INTERPOL - Coordinating law-enforcement agencies  
and legislations**

**NATO - Cyber Defense Policy and Concept**

**G8 High Tech Group - Recommendations and Best  
Practices**

**OECD, several regional organizations**

# Council of Europe

## Convention on Cyber crime (C<sup>3</sup>)

- opened for signature 2001
- entry into force 2004
- open to MS and non-MS
- 46 member states

# C<sup>3</sup>: Substantial criminal law

- ⦿ Article 2 - Illegal access
- ⦿ Article 3 - Illegal interception
- ⦿ Article 4 - Data interference
- ⦿ Article 5 - System interference
- ⦿ Article 6 - Misuse of devices
- ⦿ Article 7 - Computer-related forgery
- ⦿ Article 8 - Computer-related fraud
- ⦿ Article 9 - Offences related to child pornography
- ⦿ Article 10 - Offences related to infringements of copyright and related rights



# C<sup>3</sup>: Procedural Issues

- Preservation and disclosure of traffic data
- Search and seizure of stored computer data
- Real-time information collection
- Interception of computer data
- Jurisdiction issues
- Extradition
- Mutual assistance
- 24/7 Network

# Council of Europe

## Convention on the Prevention on Terrorism

- opened for signature 2005
- entry into force 2007
- 31 member states

## Some observations

- Soft law or insufficient number of states parties
- Different views as to whether there are gaps in international law in general
- Difficult to achieve additional consensus
- Focus to be put on ensuring the effective implementation of the conventions

# European Union

## Directives:

- ◎ Personal Data Protection
- ◎ Data Retention
- ◎ Electronic Communications
- ◎ ISP liability
- ◎ Information Society Services
- ◎ Spam
- ◎ Critical Infrastructure Protection\*

## Some observations

- Focus on common market
- No direct effect on national security issues
- Common nominator for all Member States' legal systems

# European Union

## Framework Decisions:

- Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism
- Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

### 2005/222/JHA vs C<sup>3</sup>

Article 2

Illegal access to  
information systems

Article 2 (Illegal access)

Article 3

Illegal system interference

Article 3 (System  
interference)

Article 4

Illegal data interference

Article 4 (Data Interference)

# Estonian proposal

## Article 7

### Aggravating circumstances

New paragraph 3: All member states must take the appropriate measures to ensure that offences listed in articles 2-4, directed against critical infrastructures or disturbing the provision of public services, be punishable with criminal penalties of a maximum of at least between two and five years imprisonment.

# More on cooperation and law

- Bilateral agreements provide legal basis for mutual cooperation (investigation, prosecution, extradition etc.)
- Countries with no legal coverage in the field are a good “jurisdiction shopping forum”
- International discussions do not stand in court, different arguments and legal schools need to be balanced
- Law is important, but secondary means in ensuring effective cyber security

# National Security Policy

The National Cyber Security Policy 2013 aims at

- (1) facilitating the creation of secure computing environment
- (2) enabling adequate trust and confidence in electronic transactions and
- (3) guiding stakeholders actions for the protection of cyberspace.

# The need to protect information

National Cyber Security Policy 2013 should be seen as about **protecting of information**, such as personal information, financial/banking information, sovereign data etc.

- Information empowers, and in order to empower people with information, we need to **secure the information/data**.
- There is a need to **distinguish between data which can freely flow and data which needs to be protected**.



- The “National Cyber Security Policy” has been prepared in consultation with all relevant stakeholders, user entities and public.
- This policy aims at facilitating the creation of secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholders actions for the protection of cyberspace.
- The National Cyber Security Policy document outlines a roadmap to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.
- The policy recognizes the need for objectives and strategies that need to be adopted both at the national level as well as international level.

- Vision
  - To build a secure and resilient cyberspace for citizens, businesses and Government
- Mission
  - To protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.
- Objectives
  - 1) To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

- 2) To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).
- 3) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.
- 4) To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.
- 5) To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.
- 6) To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.

- 7) To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.
- 8) To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.
- 9) To provide fiscal benefits to businesses for adoption of standard security practices and processes.
- 10) To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.
- 11) To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.
- 12) To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.
- 13) To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.
- 14) To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

# • Strategies

## A. Creating a secure cyber ecosystem

- 1) To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.
- 2) To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.
- 3) To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- 4) To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.
- 5) To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.
- 6) To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.
- 7) To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.
- 8) To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

- **B. Creating an assurance framework**

- 1) To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.
- 2) To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).
- 3) To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.
- 4) To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.
- 5) To encourage secure application / software development processes based on global best practices.
- 6) To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.
- 7) To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

- C. Encouraging Open Standards
  - 1) To encourage use of open standards to facilitate interoperability and data exchange among different products or services.
  - 2) To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.
- D. Strengthening the Regulatory framework
  - 1) To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.
  - 2) To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.
  - 3) To enable, educate and facilitate awareness of the regulatory framework.

- E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats
  - 1) To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.
  - 2) To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.
  - 3) To operationalise 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.
  - 4) To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.
  - 5) To conduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.



- F. Securing E-Governance services

- 1) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.
- 2) To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.
- 3) To engage information security professionals / organisations to assist e-Governance initiatives and ensure conformance to security best practices.

- G. Protection and resilience of Critical Information Infrastructure

- 1) To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- 2) To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.
- 3) To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.
- 4) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.
- 5) To encourage and mandate as appropriate, the use of validated and certified IT products.
- 6) To mandate security audit of critical information infrastructure on a periodic basis.
- 7) To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.
- 8) To mandate secure application / software development process (from design through retirement) based on global best practices.

- H. Promotion of Research & Development in cyber security

- 1) To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long term goals. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.
- 2) To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.
- 3) To facilitate transition, diffusion and commercialisation of the outputs of Research & Development into commercial products and services for use in public and private sectors.
- 4) To set up Centres of Excellence in areas of strategic importance for the point of security of cyber space.
- 5) To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.

- I. Reducing supply chain risks

- 1) To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.
- 2) To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.
- 3) To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.

- J. Human Resource Development

- 1) To foster education and training programs both in formal and informal sectors to support the Nation's cyber security needs and build capacity.
- 2) To establish cyber security training infrastructure across the country by way of public private partnership arrangements.
- 3) To establish cyber security concept labs for awareness and skill development in key areas.
- 4) To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

- **K. Creating Cyber Security Awareness**
  - 1) To promote and launch a comprehensive national awareness program on security of cyberspace.
  - 2) To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.
  - 3) To conduct, support and enable cyber security workshops / seminars and certifications.
- **L. Developing effective Public Private Partnerships**
  - 1) To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.
  - 2) To create models for collaborations and engagement with all relevant stakeholders.
  - 3) To create a think tank for cyber security policy inputs, discussion and deliberations.

- **M. Information sharing and cooperation**
  - 1) To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.
  - 2) To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.
  - 3) To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.
- **N. Prioritized approach for implementation**
  - To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

- Operationalisation of the Policy
  - This policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

# What is Cyber Forensics?

## ▶ **What?**

The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

## ▶ **How?**

Through the digital forensics investigation process including: **I**dentification, **P**reservation, **A**nalysis, and **P**resentation (IPAP).

## ▶ **Why?** Used in criminal investigations to identify what happened, how it happened, when it happened and the people involved.



# Relationship between Cybersecurity and Cyber Forensics

- ▶ Cybersecurity aims to protect electronic assets from breaches; whereas, cyber forensics explains how a policy became violated and who was responsible for it.

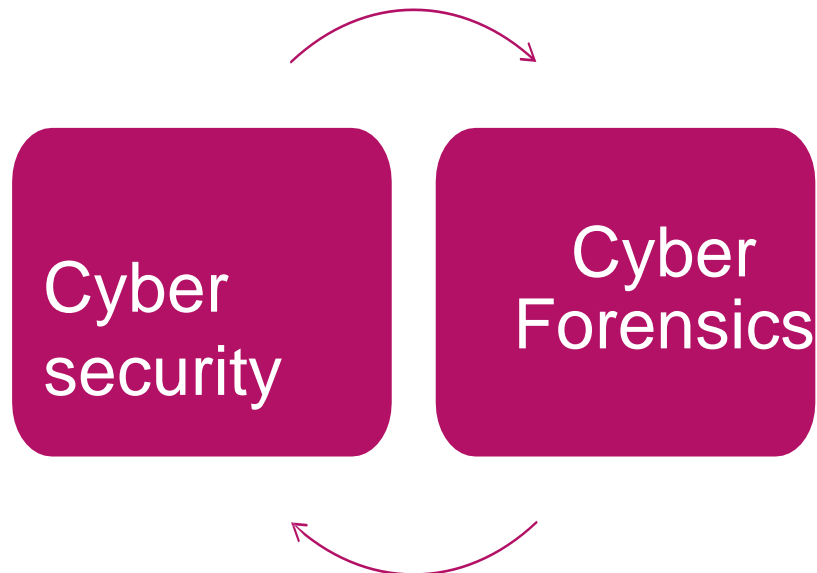


Fig. 1 Feedback cycle of Cybersecurity and Cyber Forensics

# Edmond Locard's Principle

**Locard's Principle** - Perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence; thus, every Cyber Fraud or Cyber Crime will have evidence.

## **Example:**

10 people decide to go hunting and all shoot at the same deer at the same time. The group takes the deer's life; however there is only 1 entry wound. Which hunter killed the deer?



# Historical Background of Cyber forensics

- In 1978 the State of Florida passed Fla. Stat. 815.01, the "[Florida Computer Crimes Act](#)". This law, which included legislation against the unauthorized modification or deletion of data on a computer system, and against damage to computer hardware including networks, may be the earliest American statute specifically against computer crimes. The maximum penalty for a single offense classified as a Felony of the Third Degree was:
  - "Up to 5 years of imprisonment and a fine of up to \$5,000 or any higher amount equal to double the pecuniary gain derived from the offense by the offender or double the pecuniary loss suffered by the victim."

## **1. Computer forensics**

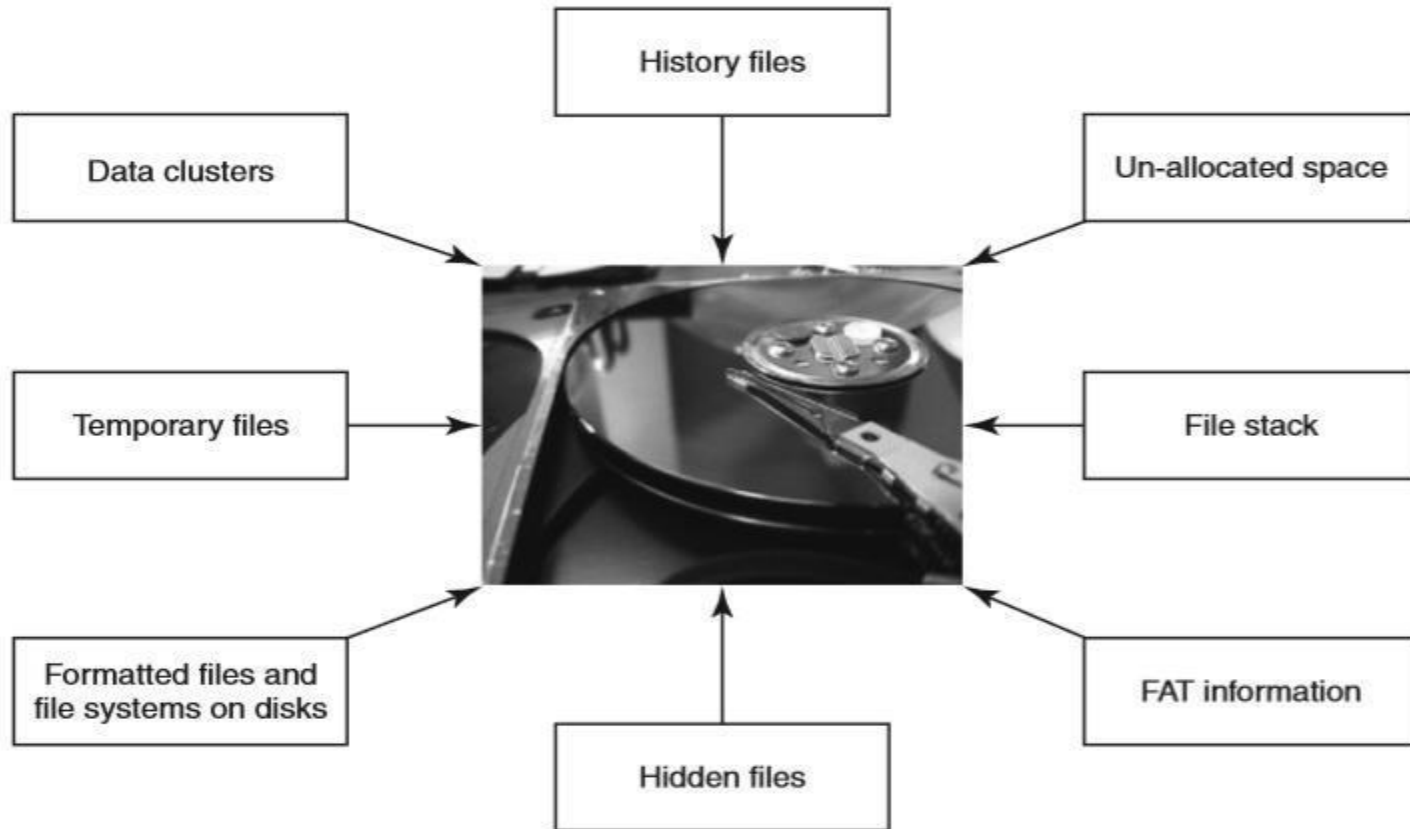
- It is the lawful and ethical seizure, acquisition, analysis, reporting and safeguarding of data and metadata derived from digital devices which may contain information that is notable and perhaps of evidentiary value to the trier of fact in managerial, administrative, civil and criminal investigations.
- In other words, it is the collection of techniques and tools used to find evidence in a computer.

## **2. Digital forensics**

- It is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.
  1. Uncover and document evidence and leads.
  2. Corroborate evidence discovered in other ways.
  3. Assist in showing a pattern of events (data mining has an application here).
  4. Connect attack and victim computers.
  5. Reveal an end-to-end path of events leading to a compromise attempt, successful or not. Extract data that may be hidden, deleted or otherwise not directly available.

- The typical scenarios involved are:
  1. Employee Internet abuse.
  2. Data leak/data breach.
  3. Industrial espionage.
  4. Damage assessment.
  5. Criminal fraud and deception cases;
  6. Criminal cases.
  7. Copyright violation

# Data seen using forensics tools. FAT means file allocation table



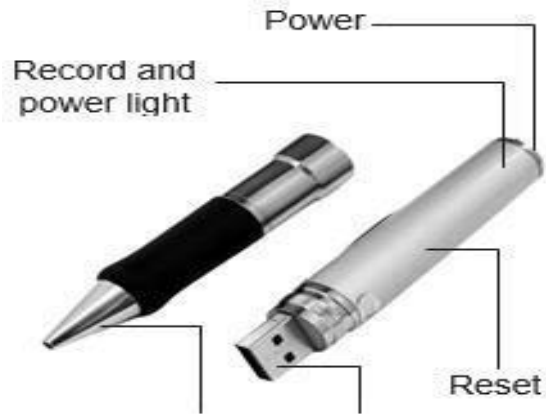
- Using digital forensics techniques, one can:
  1. Corroborate and clarify evidence otherwise discovered.
  2. Generate investigative leads for follow-up and verification in other ways.
  3. Provide help to verify an intrusion hypothesis.
  4. Eliminate incorrect assumptions.

# The Need for Computer Forensics

- The convergence of Information and Communications Technology (ICT) advances and the pervasive use of computers worldwide together have brought about many advantages to mankind. At the same time, this tremendously high technical capacity of modern computers/computing devices provides avenues for misuse as well as opportunities for committing crime.



# Fig: Hidden and miniaturized storage media



- “Fungibility” means the extent to which the components of an operation or product can be inter- changed with similar components without decreasing the value of the operation or product.
- Chain of custody means the chronological documentation trail, etc. that indicates the seizure, custody, control, transfer, analysis and disposition of evidence, physical or electronic. Chain of custody is also used in most evidence situations to maintain the integrity of the evidence
- **Chain of Custody Concept**
  1. Chain of custody is the central concept in cyber forensics/digital forensics investigation.
  2. The purpose of the chain of custody is that the proponent of a piece of evidence must demonstrate that it is what it purports to be.
  3. The chain of custody is a chronological written record of those individuals who have had custody of the evidence from its initial acquisition until its final disposition.

# Cyber forensics and Digital Evidence

- Cyber forensics can be divided into two domains:
  - 1. Computer forensics.
  - 2. Network forensics.
- As compared to the “physical” evidence, “digital evidence” is different in nature because it has some unique characteristics. First of all, digital evidence is much easier to change/manipulate! Second, “perfect” digital copies can be made without harming original.

# The Rules of Evidence

- It was mentioned in that the Indian IT Act amended the Indian Evidence Act. According to the “Indian Evidence Act 1872,” “Evidence” means and includes:
  1. All statements which the court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, are called oral evidence.
  2. All documents that are produced for the inspection of the court are called documentary evidence.
- Paper evidence, the process is clear and intuitively obvious. Digital evidence by its very nature is invisible to the eye. Therefore, the evidence must be developed using tools other than the human eye.

- There are number of contexts involved in actually identifying a piece of digital evidence:
- 1. Physical context: It must be definable in its physical form, that is, it should reside on a specific piece of media.
- 2. Logical context: It must be identifiable as to its logical position, that is, where does it reside relative to the file system.
- 3. Legal context: We must place the evidence in the correct context to read its meaning. This may require looking at the evidence as machine language, for example, American Standard Code for Information Interchange (ASCII).

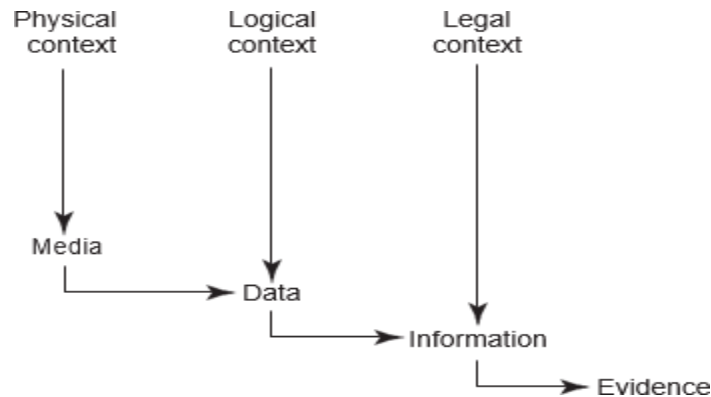


Fig: Path of the digital evidence.

- Following are some guidelines for the (digital) evidence collection phase:
  1. Adhere to your site's security policy and engage the appropriate incident handling and law enforcement personnel.
  2. Capture a picture of the system as accurately as possible.

# Forensics Analysis of E-Mail

- It was mentioned how criminals can use fake mails for various cybercrime offenses.
- There are tools available that help create fake mails. Forensics analysis of E-Mails is an important aspect of cyber forensics analysis, it helps establish the authenticity of an E-Mail when suspected.
- Mail server software is a network server software that controls the flow of E-Mail and the mail client software helps each user read, compose, send and delete messages.
- E-Mail tracing is done by examining the header information contained in E-Mail messages to determine their source.

# Digital Forensics Life Cycle

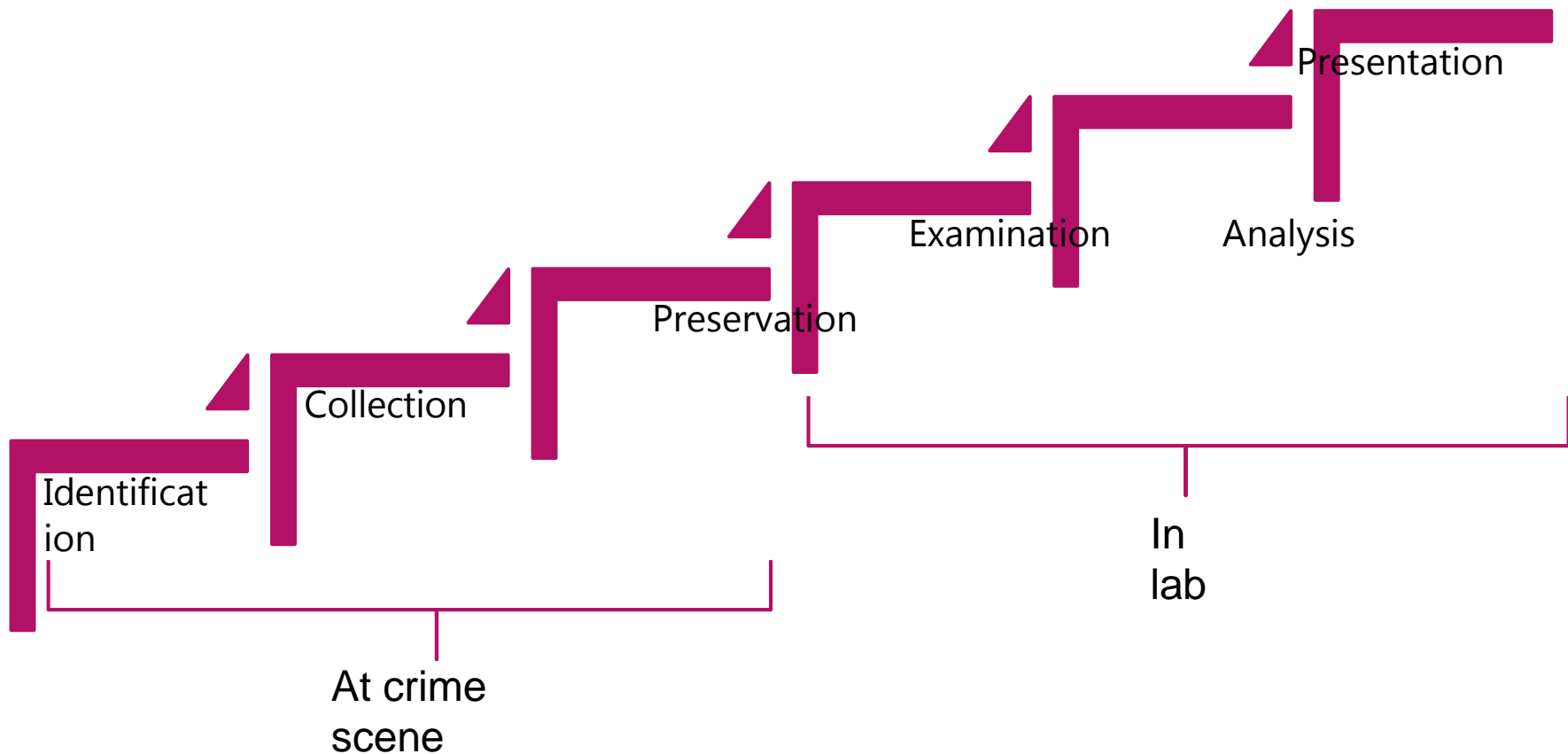
- As per FBI's (Federal Bureau of Investigation) view, digital evidence is present in nearly every crime scene. That is why law enforcement must know how to recognize, seize, transport and store original digital evidence to preserve it for forensics examination.
  - 1. Is admissible.**
  - 2. Is authentic.**
  - 3. Is complete.**
  - 4. Is reliable.**
  - 5. Is understandable and believable.**
- Let us now understand what is involved in the digital forensics process.



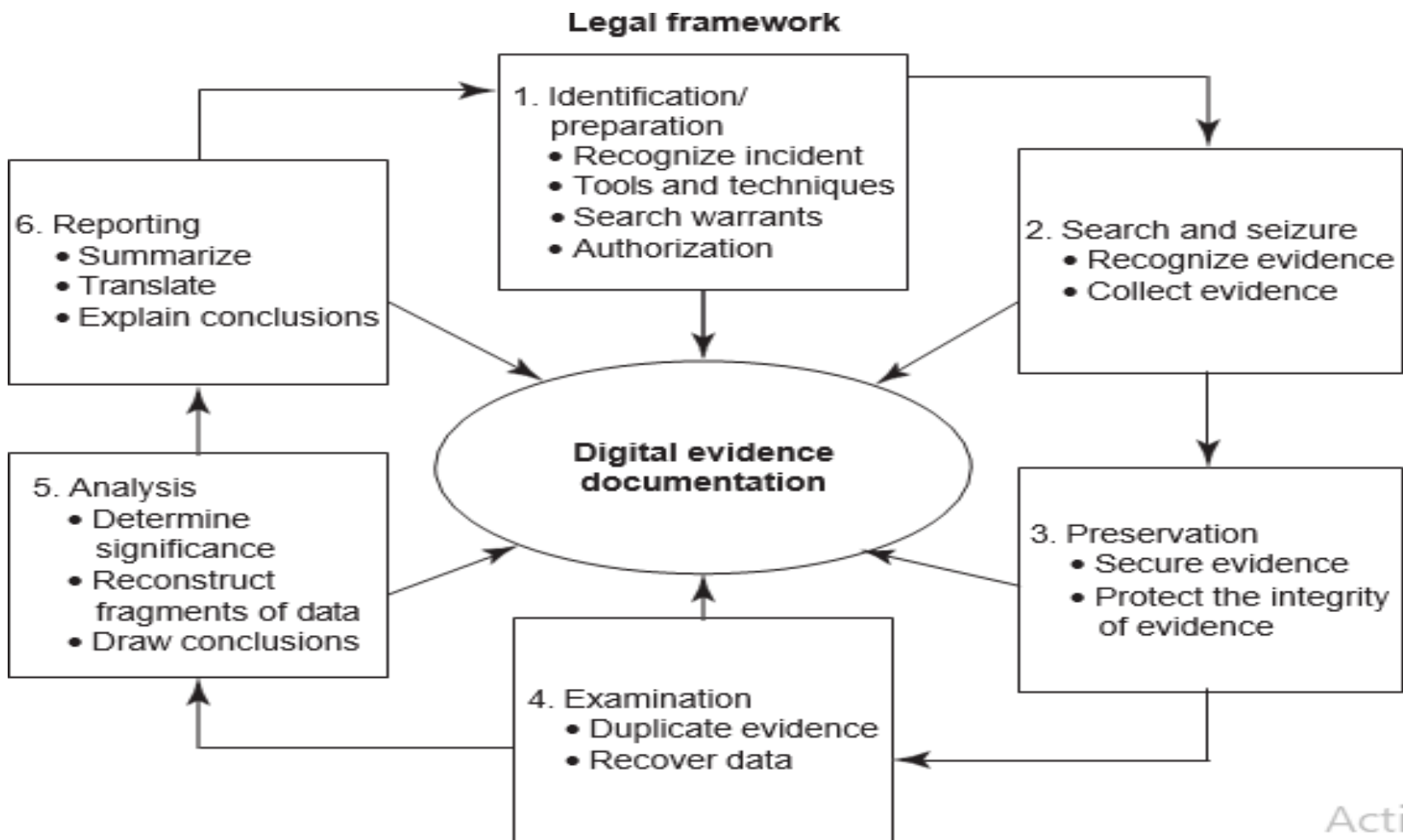
# The Digital Forensics Process

- The digital forensics process needs to be understood in the legal context starting from preparation of the evidence to testifying. Digital forensics evidence consists of exhibits, each consisting of a sequence of bits, presented by witnesses in a legal matter to help jurors establish the facts of the case and support or refute legal theories of the case.

# Digital Forensics Investigation Process Model



**Fig: Process model for understanding a seizure and handling of forensics evidence legal framework.**



# The Phases in Computer Forensics/Digital Forensics

- The investigator must be properly trained to perform the specific kind of investigation that is at hand.
- Tools that are used to generate reports for court should be validated.
- There are many tools to be used in the process.
- One should determine the proper tool to be used based on the case. Broadly speaking, the forensics life cycle involves the following phases:
- **1. Preparation and identification** : Case briefings engagement terms, interrogatories, spoliation prevention, disclosure and discovery planning, discovery requests.
- **2. Collection and recording** : Drive imaging, indexing, profiling, search plans, cost estimates, risk analysis.
- **3. Storing and transporting**
- **4. Examination/investigation** : Triage images, data recovery, keyword searches, hidden data review, communicate, iterate
- **5. Analysis, interpretation and attribution**
- **6. Reporting** : Oral vs. written, relevant document production, search statistic reports, chain of custody reporting, case log reporting
- **7. Testifying: Testimony preparation, presentation preparation, testimony.**
- To mention very briefly, the process involves the following activities:

- **Preparing for the Evidence and Identifying the Evidence**

- **Collecting and Recording Digital Evidence**

Digital evidence can be collected from many sources. Obvious sources include computers, cell phones, digital cameras, hard drives, CD-ROM, USB memory devices and so on. Non-obvious sources include settings of digital thermometers, black boxes inside automobiles, RFID tags and webpages (which must be preserved as they are subject to change).

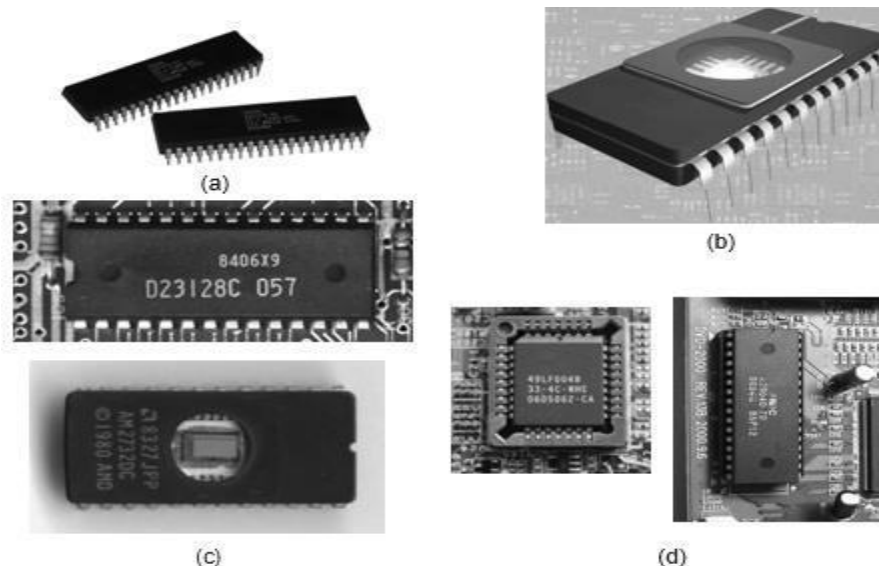
# Fig: Media that can hold digital evidences



# • Storing and Transporting Digital Evidence

The following are specific practices that have been adopted in the handling of digital evidence:

1. Image computer media using a write-blocking tool to ensure that no data is added to the suspect device;
2. establish and maintain the chain of custody.



**Fig: Embedded memories inside computer. (a) Read-only memory (ROM) chips; (b) erasable programmable read-only memory (EPROM) chip; (c) programmable read-only memory (PROM) chips; (d) electrify erasable programmable read-only memory (EEPROM) chips.**

Some of the most valuable information obtained in the course of a forensics examination will come from the computer user. An interview with the user can yield valuable information about the system configuration, applications, encryption keys and methodology. Forensics analysis is much easier when analysts have the user's passphrases to access encrypted files, containers and network servers. As a general rule, one should not examine digital information unless one has the legal authority to do so. Amateur forensics examiners should keep this in mind before starting any unauthorized investigation.

For the purpose of digital evidence examination, "imaging of electronic media" (on which the evidence is believed to be residing) becomes necessary.

- **Analysis, Interpretation and Attribution**

Analysis, interpretation and attribution of evidence are the most difficult aspects encountered by most forensics analysts. In the digital forensics arena, there are usually only a finite number of possible event sequences that could have produced evidence.

Examples of common digital analysis types include:

1. Media Analysis
2. Media Management Analysis
3. File System Analysis
4. Application Analysis
5. Network Analysis
6. OS Analysis
7. Executable Analysis
8. Image Analysis
9. Video Analysis



- **Reporting**

The following are the broad-level elements of the report

1. Identity of the reporting agency
2. Case identifier or submission number
3. Case investigator
4. Identity of the submitter
5. Date of receipt
6. Date of report
7. Descriptive list of items submitted for examination, including serial number, make and model
8. Identity and signature of the examiner
9. Brief description of steps taken during examination, such as string searches, graphics image searches and recovering erased files
10. Results/conclusions.

- **Testifying / Presentation**

This phase involves presentation and cross-examination of expert witnesses. Depending on the country and legal frameworks in which a cybercrime case is registered, certain standards may apply with regard to the issues of expert witnesses.

- **Network Forensics**

Network forensics professionals need to understand how wireless networks work and the fundamentals of related technology.

Wireless forensics is a discipline included within the computer forensics science, and specifically, within the network forensics field. The goal of wireless forensics is to provide the methodology and tools required to collect and analyze (wireless) network traffic that can be presented as valid digital evidence in a court of law.

- **Approaching a Computer Forensics Investigation**
  - From the discussion so far, we can appreciate that computer forensics investigation is a detailed science.
  - The phases involved are as follows:
    1. Secure the subject system (from tampering or unauthorized changes during the investigation);
    2. take a copy of hard drive/disk (if applicable and appropriate);
    3. identify and recover all files (including deleted files);
    4. access/view/copy hidden, protected and temp files;
    5. study “special” areas on the drive (e.g., the residue from previously deleted files);
    6. investigate the settings and any data from applications and programs used on the system;
    7. consider the system as a whole from various perspectives, including its structure and overall contents;
    8. consider general factors relating to the user’s computer and other activity and habits in the context of the investigation;
    9. create detailed and considered report, containing an assessment of the data and information collected.

- **Typical Elements Addressed in a Forensics Investigation Engagement Contract**

1. Authorization
2. Confidentiality
3. Payment
4. Consent and acknowledgment
5. Limitation of liability

- Laboratory responsible for any accidental damages to the data or equipment in its possession including but not limited to surface scratches, deformations and cracks.

**1. Customer's representation: Customer needs to warrant the forensics laboratory that he/she is the owner of, and/or has the right to be in possession of, all equipment/data/media furnished to the laboratory and that collection, possession, processing and transfer of such equipment/data/media are in compliance with data protection laws to which customer is subject to.**

**2. Legal aspects/the law side: Both the parties need to agree that the agreement shall be governed by prevailing law in every particular way including formation and interpretation and shall be deemed to have been made in the country where the contract is signed.**

- 3. Data protection: The computer forensics laboratory (engaged in the investigation) will hold the information that the customer has given verbally, electronically or in any submitted form for the purpose of the forensics investigation to be carried out as per contracted services from the forensics laboratory.
- 4. Waiver/breach of contract: The waiver by either party of a breach or default of any of the provisions on this agreement by either party shall not be construed as a waiver of any succeeding breach of the same or other provisions, nor shall any delay or omission on the part of either party to exercise or avail itself of any right, power or privilege that it has, or may have hereunder operate as a waiver of any breach or default by either party.

# • Solving a Computer Forensics Case

1. Prepare for the forensics examination.
2. Talk to key people to find out what you are looking for and what the circumstances surrounding the case are.
3. If you are convinced that the case has a sound foundation, start assembling your tools to collect the data in question. Identify the target media.
4. Collect the data from the target media. You will be creating an exact duplicate image of the device in question. To do this, you will need to use an imaging software application like the commercial in Case or the open-source Sleuth Kit/Autopsy.
5. To extract the contents of the computer in question, connect the computer you are investigating to a portable hard drive or other storage media and then boot the computer under investigation according to the directions for the software you are using.
6. When collecting evidence, be sure to check E-Mail records as well. Quite often, these messages yield a great deal of information.
7. Examine the collected evidence on the image you have created. Document anything that you find and where you found it.
8. Analyze the evidence you have collected by manually looking into the storage media and, if the target system has a Windows OS, check the registry.
9. Report your findings back to your client. Be sure to provide a clear, concise report; this report may end up as evidence in a court case.

- **Setting up a Computer Forensics Laboratory**  
**Understanding the Requirements**
- There are four broad types of requirements, namely, the physical space, the hardware equipment, the software tools and the forensics procedures to be followed to aid those involved in the cybercrime investigation.



**Fig: Cyber forensics laboratory – 1**



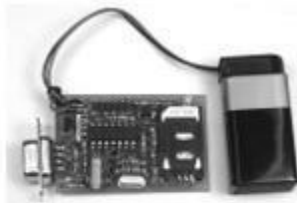
**Fig: Cyber forensics laboratory – 2**

-



- Apart from the physical space requirement, another key requirement for a computer forensics laboratory is the hardware items. The laboratory requires a number of computers, including a network server with a large storage capacity (preferably configured for the standard removable hard drives).

**Fig: (a) SIM card reader, (b) iButtons, (c) flash memory, (d) SIM card.**



(a)



(b)



(c)



(d)

- On the software side, there are several requirements for setting up a forensics laboratory. The standard forensics software package, such as EnCase, Web Case, Forensics Tool Kit, Password Recovery Tool Kit, etc. are expensive products.
- The main issues that are attacked when evidence is presented in a court of law are credentials and methodology. In some countries, the court may prefer the forensics evidence from government appointed and/or neutral party laboratories rather than the evidence from private agencies where opportunities for manipulation / exploitation are perceived.

- **Computer Forensics and Steganography**

- Steganography is the art of information hiding. The threat raised by steganography is very real. Its use is not easy to detect or intercept, as the information does not need to be broadcast across the Internet. the hidden message can reside unsuspectingly on a website, for example, and can be viewed from around the world.
- Steganography is the art of information hiding. The threat raised by steganography is very real. Its use is not easy to detect or intercept, as the information does not need to be broadcast across the Internet. The hidden message can reside unsuspectingly on a website, for example, and can be viewed from around the world.

- **Rootkits**

- The term rootkit is used to describe the mechanisms and techniques whereby malware including viruses, Spyware and Trojans attempt to hide their presence from Spyware blockers, antivirus and system management utilities

- **Information Hiding**
- **Relevance of the OSI 7 Layer Model to Computer Forensics**
- The OSI 7 Layer Model is useful from computer forensics perspective because it addresses the network protocols and network communication processes. The basic familiarity with the OSI 7 Layer Model is assumed for the discussion in this section.

# Fig: The OSI 7 Layer Model with Internet Protocols.

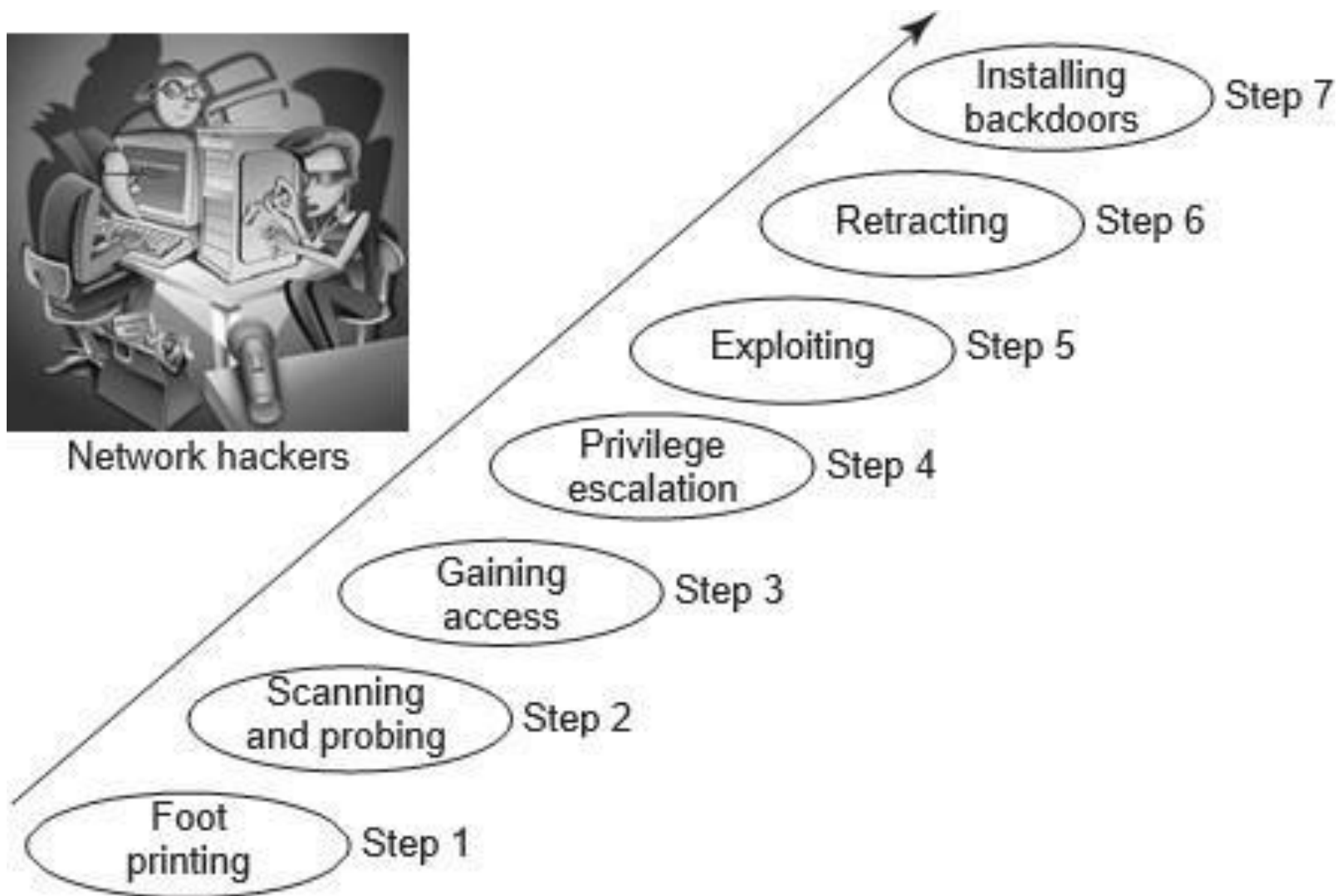
← Protocols, browser, Calls and browser-based languages →

OSI layers						
Layer 7	Application	Ping (command)	NFS	Web browser	E-Mail client	Windows file and print sharing
Layer 6	Presentation		XDR	HTML	MIME	
Layer 5	Session		RPC	HTTP	SMTP	RPC and SMB
Layer 4	Transport	ICMP	UDP	TCP		NetBEUI
Layer 3	Network	IP				
Layer 2	Datalink	802.2				
Layer 1	Physical	Ethernet				

# Fig: Network hacking steps



Network hackers



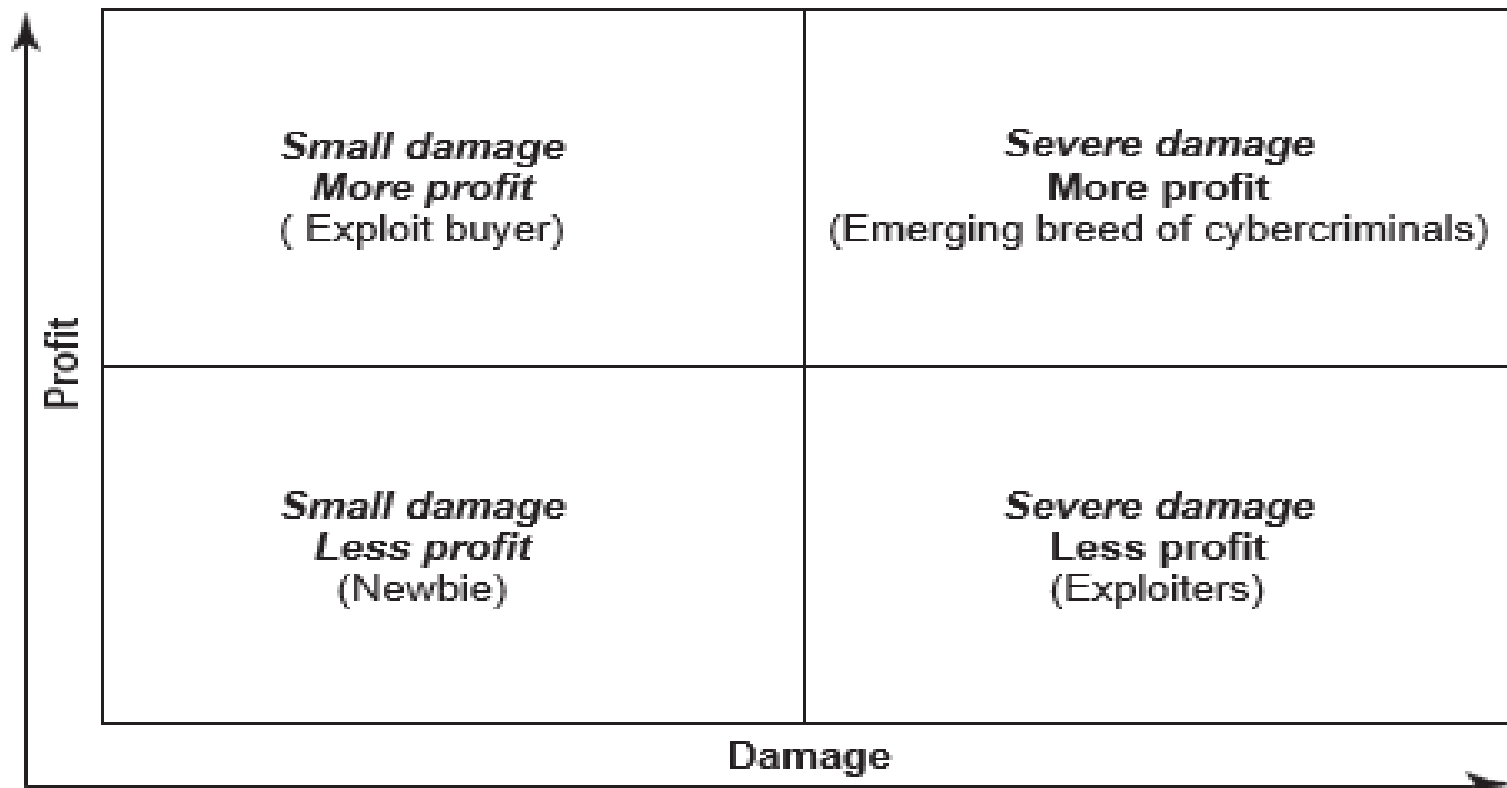
## **Step 1: Foot Printing**

- Foot printing includes a combination of tools and techniques used to create a full profile of the organization's security posture. These include its domain names, IP addresses and network blocks.

## **Step 2: Scanning and Probing**

- The hacker will typically send a ping echo request packet to a series of target IP addresses. As a result of this exploratory move by the hacker, the machines assigned to one of these IP address will send out echo response thereby confirming that there is a live machine associated with that address.
- Similarly, a TCP scan sends a TCP synchronization request to a series of ports and to the machines that provide the associated service to respond.

# Fig. Hacker categories (profit and damage).





### **Step 3: Gaining Access**

- The hacker's ultimate goal is to gain access to your system so that he/she can perform some malicious action, such as stealing credit card information, downloading confidential files or manipulating critical data.

### **Step 4: Privilege**

- When a hacker gains access to the system, he will only have the privileges granted to the user or account that is running the process that has been exploited.

### **Step 5: Exploit**

- Gaining root access gives the hacker full control on the network. Every hacker seems to have his/her own reasons for hacking. Some hackers do it for fun or a challenge, some do it for financial gain and others do it to "get even".

### **Step 6: Retracting**

- There are many reasons that drive cybercriminals to hacking.

### **Step 7: Installing Backdoors**

- Finally, most hackers will try creating provisions for entry into the network/hacked system for later use. This, they will do by installing a backdoor to allow them access in the future.

## **Computer Forensics from Compliance Perspective**

- With the rampant use of the Internet, there is so much at stake; corporate data is not safe anymore given that almost all information assets lie on the corporate networks. We are in the era of Net-centric digital economy.
- Criminals can gather small pieces about you, about your confidential data to generate what is known as “digital persona,” that is, they keep track about your Internet activities, what resides on your corporate networks, etc.

## **The Regulatory Perspective for Forensics at the International Level**

- These laws/regulations specify investigation and response to security breaches or policy violations. Computer forensics makes it easier to meet these requirements.

- **These laws/legislations become relevant in the context of forensics with cybercrimes.**

**1. The Sarbanes Oxley Act (SOX): The Act was enacted to fight corporate fraud.**

**2. California SB 1386**

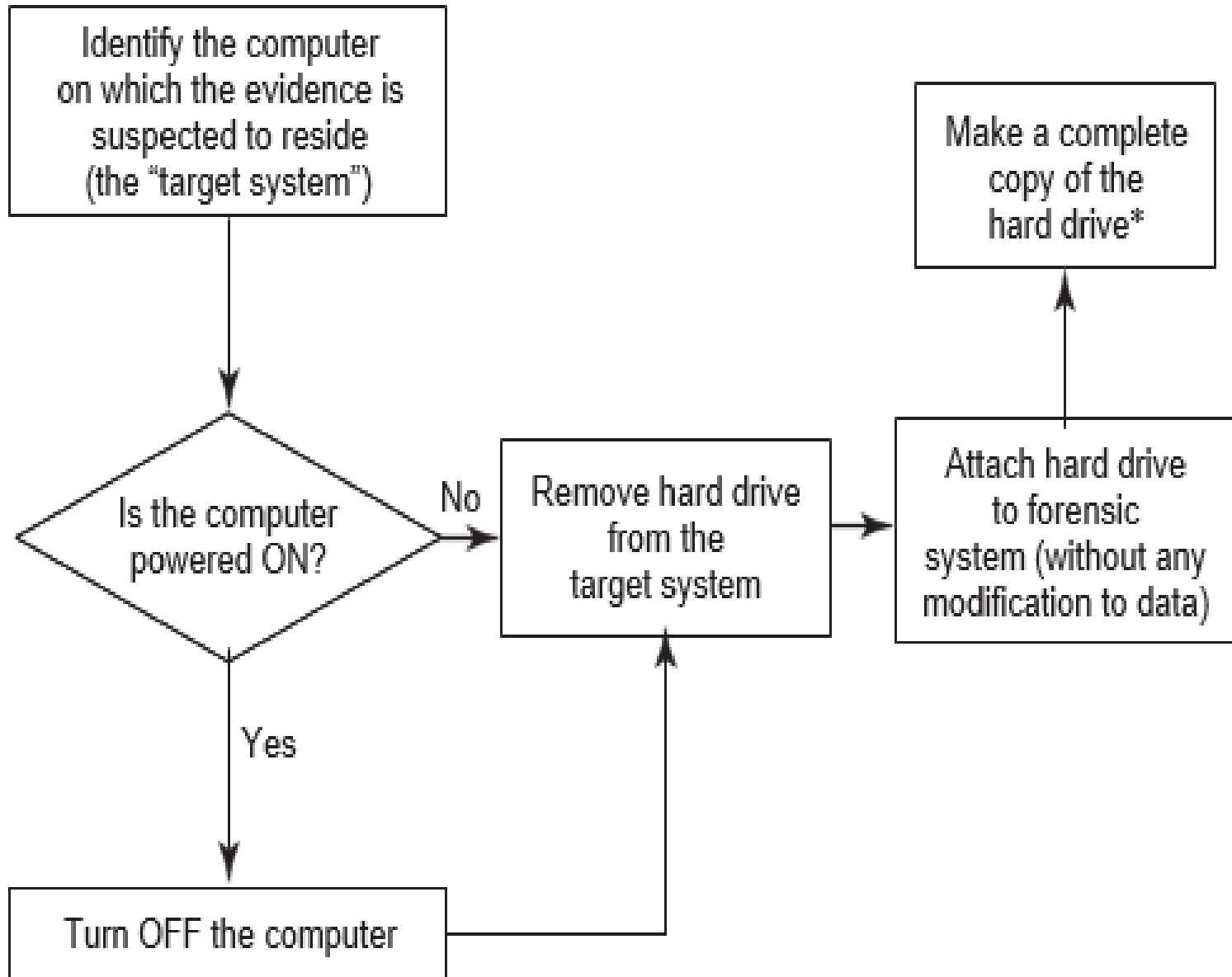
**3. Gramm-Leach Bliley Act (GLBA)**

The Safeguards Rule of GLB calls for financial institutions to:

- a) Ensure the security and confidentiality of customer information;
- b) Protect against any anticipated threats or hazards to the security or integrity of such information;
- c) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

**4. HIPAA (Health Insurance Portability and Accountability Act of 1996)**

- HIPAA has the primary goal for healthcare providers to improve the privacy and security of their clients' medical information.
- **Fig: Traditional approach to forensics analysis. \*denotes tools/devices mentioned**



# Forensics Investigation

The basic steps to a forensics investigation are as follows:

1. *Prepare*—Specific forensics training, overarching corporate policies and procedures, as well as practice investigations and examinations will prepare you for an “event.” Specialized forensics or incident handling certifications are considered of great value for forensics investigators.
2. *Identify*—When approaching an incident scene—review what is occurring on the computer screen. If data is being deleted, pull the power plug from the wall; otherwise perform real-time capture of system “volatile” data first.
3. *Preserve*—Once the system-specific “volatile” data is retrieved, then turn off machine, remove it from scene, and power it up in an isolated environment. Perform a full system bit-stream image capture of the data on the machine, remembering to “hash” the image with the original data for verification purposes.
4. *Select* —Once you have a verified copy of the available data, start investigation of data by selecting potential evidence files, datasets, and locations data could be stored. Isolate event-specific data from normal system data for further examination.

5. *Examine*—Look for potential hidden storage locations of data such as slack space, [unallocated space](#), and in front of [File Allocation Table](#) (FAT) space on hard drives. Remember to look in registry entries or root directories for additional potential indicators of data storage activity.
6. *Classify*—Evaluate data in potential locations for relevance to current investigation. Is the data directly related to case, or does it support events of the case, or is it unrelated to the case?
7. *Analyze*—Review data from relevant locations. Ensure data is readable, legible, and relevant to investigation. Evaluate it for type of evidence: Is it direct evidence of alleged issue or is it related to issue?
8. *Present*—Correlate all data reviewed to investigation papers (warrants, corporate documents, etc.). Prepare data report for presentation—either in a court of law or to corporate officers.

# Challenges of Computer Forensics

- A microcomputer may have 60-GB or more storage capacity.
- There are more than 2.2 billion messages expected to be sent and received (in US) per day.
- There are more than 3 billion indexed Web pages world wide.
- There are more than 550 billion documents on line.
- Exabytes of data are stored on tape or hard drives.
  - (Source: Marcella, Albert, et al, *Cyber Forensic*, 2002.)

# Challenges of Computer Forensics (continued)

- How to collect the specific, probative, and case-related information from very large groups of files?
  - Link analysis
  - Visualization
- Enabling techniques for lead discovery from very large groups of files:
  - Text mining
  - Data mining
  - Intelligent information retrieval



# Challenges of Computer Forensics (continued)

- Computer forensics must also adapt quickly to new products and innovations with valid and reliable examination and analysis techniques.



# FORENSIC AUDIT

2.21%	-15.88%	2.58%	5.41%
-4.88%	2.94%	-2.28%	2.28%
0.00%	-17.14%	0.07%	0.07%
-0.40%	-20.88%	-3.54%	1.1%
-5.52%	21.74%	0.0%	0.0%
8.20%	17.14%	0.0%	0.0%
0.00%	0.0%	0.0%	0.0%
0.0%	2.50%	0.0%	0.0%
0.0%	17.14%	0.0%	0.0%
1.54%	30.38%	0.0%	0.0%
4.17%	21.74%	0.0%	10.05%
-3.43%	25.00%	0.0%	-4.02%
-2.98%	31.43%	0.0%	-15.27%
1.53%	0.0%	-0.23%	0.40%
0.0%	0.0%	-5.57%	8.15%
0.0%	0.81%	-6.13%	1.58%
0.0%	20.16%	-7.77%	0.0%
0.48%	-22.15%	0.00%	1.57%
-2.38%	8.52%	14.53%	0.0%
1.06%	-0.79%	-4.57%	-5.21%
0.00%	32.00%	6.55%	2.34%
3.30%	-17.58%	-1.70%	3.24%
-0.83%	-38.24%	-12.44%	-2.17%
7.53%	14.29%	-2.03%	-4.55%
7.32%	21.58%	7.98%	9.44%
0.0%	23.03%	-2.47%	-8.47%
0.0%	0.0%	0.0%	15.0%
2.40%	0.0%	4.91%	0.0%
-7.02%	64.17%	0.00%	0.0%
1.82%	-30.32%	0.45%	0.45%
-7.12%	-26.62%	-1.33%	-1.33%
14.87%	-11.05%	2.70%	2.70%
18.89%	0.50%	-7.00%	-7.00%
0.0%	-9.50%	0.0%	0.0%
0.0%	0.0%	0.0%	0.0%

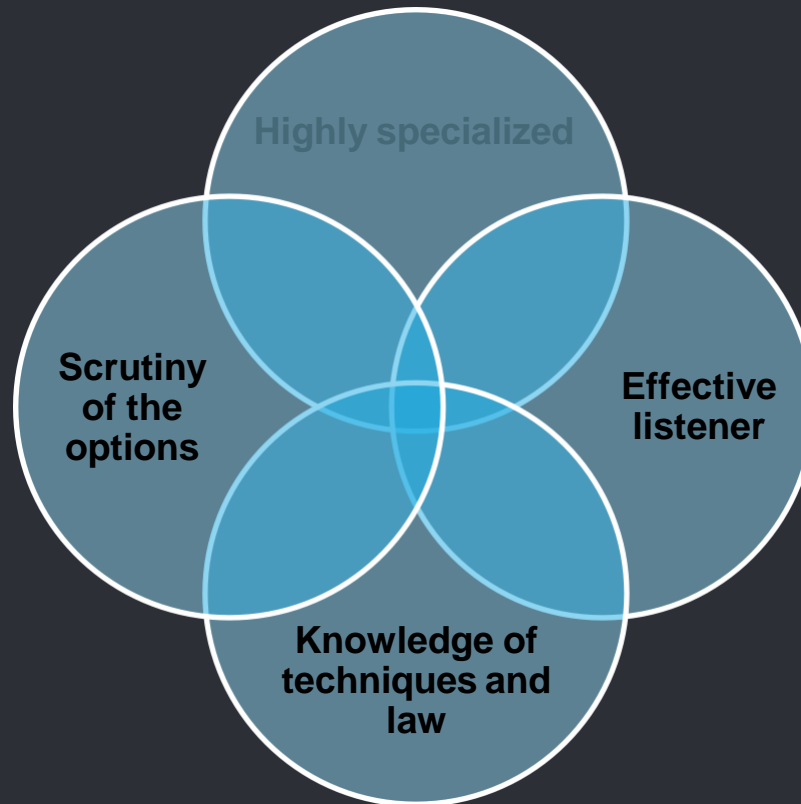
Account	Balance	Change
CASH	0	0
DEBIT	2000	-2000
CREDIT	7000	7000
SALES	5000	5000
EXPENSES	4000	-4000
TOTAL	0	0

## WHAT IS FORENSIC AUDIT ?

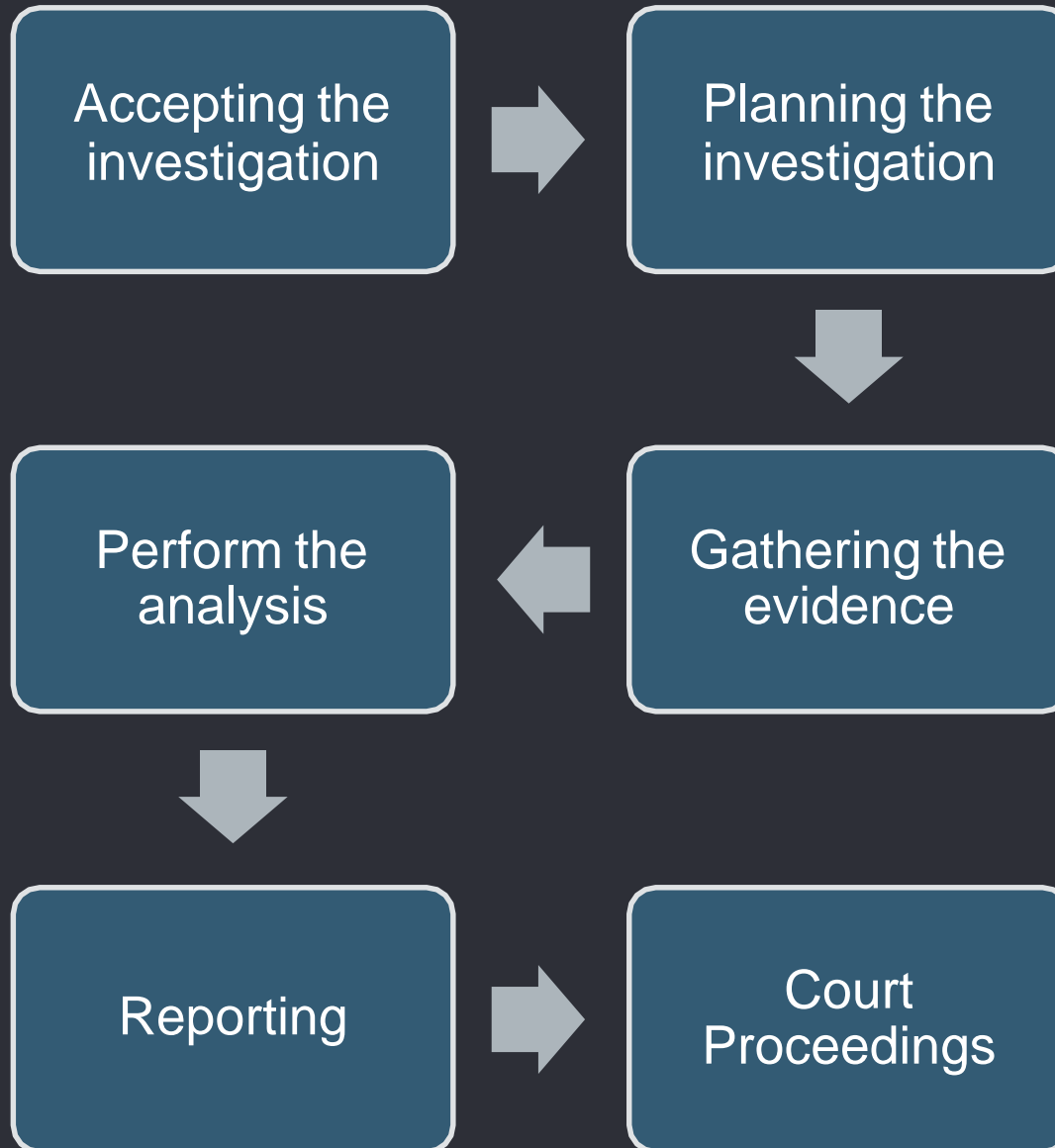
- A forensic audit, refers to the application of accounting methods for detection and gathering evidence of frauds, embezzlement, or any other such white-collar crime.
- It is an examination of a company's financial records to derive evidence which can be used in a court of law or legal proceeding.
- The failure of some formerly prominent public companies such as Enron, WorldCom, Xerox Corporation and Satyam Computer Services fueled the prominence of forensic auditing

## FORENSIC AUDITORS

- They are retained by banks, courts, business communities, police forces, lawyers, insurance companies, government regulatory bodies and organizations.



# HOW IS FORENSIC AUDIT INVESTIGATION CONDUCTED ?





## **Step 1– Accepting the Investigation**

The firm must ascertain whether or not they have the necessary tools, skills and expertise to go forward with such an investigation. They need to do an assessment of their own training and knowledge of fraud detection and legal framework

## **Step 2 – Planning the Investigation**

The auditor(s) must carefully ascertain the goal of the audit so being conducted, and to carefully determine the procedure to achieve it, through the use of effective tools and techniques. Planning also includes the identification of the best mode to gather evidence.



## Step 3 – Gathering the evidence

In forensic auditing specific procedures are carried out in order to produce evidence. The investigators can use the following techniques to gather evidence :

- Testing controls which identifies the weaknesses,
- Using analytical procedures to compare trends over time
- Applying computer-assisted audit techniques,
- Discussions and interviews with employees
- Substantive techniques such as reconciliations, cash counts and reviews of documentation.

## **Step 4 – Perform the analysis**

The actual analysis performed may involve calculating economic damages, summarizing a large number of transactions, tracing of assets, present value considerations

## **Step 5 – Reporting**

After investigating and gathering evidence, the investigating team is expected to give a report of the findings of the investigation, and also the summary of the evidence and conclusion about the loss suffered due to the fraud.

## **Step 6 – Court Proceedings**

The last stage expands over those audits that lead to legal proceedings. The auditors are called to the Court, and also included in the advocacy process.



# TYPES OF INVESTIGATIONS UNDER FORENSIC AUDIT

## Asset Misappropriation

- This includes misappropriation of cash, raising fake invoices, payments made to non-existing suppliers or employees
- It happens when people who are entrusted to manage the assets of an organization, steal from it.
- The direct hit is on the cash flow of the organization.



# TYPES OF INVESTIGATIONS UNDER FORENSIC AUDIT

## Corruption

Corruption is a major obstacle at corporate levels, and also to socio-economic development. It can surface in various forms such as -

- Bribery
- Extortion
- Conflict of interest



# TYPES OF INVESTIGATIONS UNDER FORENSIC AUDIT

## Financial Statement Fraud (FSF)

- Financial statement fraud is the deliberate misrepresentation, misstatement or omission of data for the purpose of misleading the reader and creating a false impression of an organization's financial strength.
- The common practice is deferring revenues or expense in a different time period to give the appearance of consistent earnings or growth.



## SATYAM CASE



- 7561 fake invoices
- Inflated receivables
- Fake Fixed Deposit Receipts were printed
- Bank guarantees were manipulated
- Fake bank balance statements of BNP Paribas, HSBC, ICICI Bank and Citibank

# ● FORENSIC AUDIT TECHNIQUES

## ○ General Audit Techniques

Testing defenses - A good forensic audit technique is to attempt to circumvent these defenses yourself. This technique requires you to put yourself in the shoes of the suspect and think accordingly.

## Statistical and Mathematical Techniques

- Trend Analysis - Careful review of the historical norms
- Ratio Analysis – Analysis of ratios report on the fraud health by identifying the possible symptoms of the fraud.

# ● FORENSIC AUDIT TECHNIQUES

## Technology based/ digital forensic techniques

Every transaction leaves a digital footprint in the computer driven society. Many digital enabled forensic tools are available to assist the auditor such as –

cross drive analysis, live analysis, Encase, MD5, Tracking log files, PC system log, Steganography, Free log tools.

## Computer aided audit tools (CAATs)

It is the practice of using computers to automate the IT audit processes. The CAAT tool supports the forensic accounting in which larger amount can be diverted to the analytical form and it also prompts where the tool detects the fraud..

# FORENSIC AUDIT TECHNIQUES

## Data Mining

Data mining is an analysis process used to examine data sets or metadata to identify patterns, anomalies, and trends to answer business queries and provide predictive value for future events. It incorporates algorithms to explore, analyze, classify, relate, and partition data sets



# FORENSIC AUDIT TECHNIQUES

## Software and tools

Generalized audit software is a category of CAAT to undertake data extraction, summarization and analytical skills. Currently the latest version of generalized audit software includes the audit command language, interactive data extraction and analysis (IDEA) and Panaudit .

Due to the shortcomings of generalized audit software, common software tools have become more popular over the time period. Spreadsheets like Ms Excel, Lotus etc, RDBMS like MsAccess etc and report writers like Crystal reports etc are few examples of CST.





# FORENSIC AUDIT IN THE CURRENT SCENARIO

# FORENSIC AUDIT IN THE NIRAV MODI CASE

A staggering 30 banks will be a part of the forensic audit, besides Punjab National Bank, to trace and track the chain of money movement

It eventually ended up as a gigantic **Rs 11,400 crore** Indian banking fraud.

Its outcome will be used as evidence in court to prosecute the key perpetrator Nirav Modi and his firms and Mehul Choksi, promoter, Gitanjali Group.

# RBI GUIDELINES



As per RBI's master direction on frauds, revised in July 2017,

In case an account is classified as a **fraud** and falls under **multiple banking arrangements**, the account should be red flagged by all banks, initiate a forensic audit and lodge complaints with the CBI and law enforcement agencies.

This process should be completed within six months.

**UNIT -III: Cybercrime Mobile and Wireless Devices:**

1. Introduction,
2. Proliferation (Growth) of Mobile and Wireless Devices,
3. Trends in Mobility,
4. Credit Card Frauds in Mobile and Wireless Computing Era,
5. Security Challenges Posed by Mobile Devices,
6. Registry Settings for Mobile Devices,
7. Authentication Service Security,
8. Attacks on Mobile/Cell Phones,
9. Mobile Devices: Security Implications for Organizations,
10. Organizational Measures for Handling Mobile,
11. Organizational Security Policies and Measures in Mobile Computing Era,
12. Laptops.

## Introduction

- In this modern era, the rising importance of *electronic gadgets* (i.e., mobile hand-held devices) – which became an integral part of business, providing connectivity with the Internet outside the office – brings many challenges to secure these devices from being a victim of cybercrime.
- In the recent years, the use of laptops, personal digital assistants (PDAs), and mobile phones has grown from limited user communities to widespread desktop replacement and broad deployment.
- By the end of 2008 around 1.5 billion individuals around the world had the Internet access.
- In November 2007, mobile phone users were numbered 3.3 billion, with a growing proportion of those mobile devices enabled for the Internet access.
- The complexity of managing these devices outside the walls of the office is something that the information technology (IT) departments in the organizations need to address.
- Remote connection has extended from fixed location dial-in to wireless-on-the-move, and smart hand-held devices such as PDAs have become networked, converging with mobile phones.
- Furthermore, the maturation of the PDA and advancements in cellular phone technology have converged into a new category of mobile phone device: the *Smartphone*.
- **Smartphones** combine the best aspects of mobile and wireless technologies and blend them into a useful business tool.
- Although IT departments of organizations as yet are not swapping employees' company- provided PDAs (as the case may be) for the Smartphones, many users may bring these devices from home and use them in the office.
- Thus, the larger and more diverse community of mobile users and their devices increase the demands on the IT function to secure the device, data and connection to the network, keeping control of the corporate assets, while at the same time supporting mobile user productivity.
- Clearly, these technological developments present a new set of security challenges to the global organizations.

## Proliferation (Growth) of Mobile and Wireless Devices

- Today, incredible advances are being made for mobile devices.
- The trend is for smaller devices and more processing power.
- A few years ago, the choice was between a wireless phone and a simple PDA. Now the buyers have a choice between high-end PDAs with integrated wireless modems and small phones with wireless Web-browsing capabilities.
- A simple hand-held mobile device provides enough computing power to run small applications, play games and music, and make voice calls.
- As the term “mobile device” includes many products. We first provide a clear distinction among the key terms: mobile computing, wireless computing and hand-held devices.
- Let us understand the concept **of mobile computing** and the various types of devices.

## Mobile computing

Mobile computing is “taking a computer and all necessary files and software out into the field.” Many types of mobile computers have been introduced since 1990s.

- They are as follows:

**1. Portable computer:** It is a *general-purpose computer that can be easily moved from one place to another*, but cannot be used while in transit, usually because it requires some “setting-up” and an AC power source.

**2. Tablet PC:** It lacks a keyboard, is shaped like a slate or a paper notebook and has features of a touch screen with a stylus and handwriting recognition software. Tablets may not be best suited for applications requiring a physical keyboard for typing, but are otherwise capable of carrying out most tasks that an ordinary laptop would be able to perform.

**3. Internet tablet:** It is the Internet appliance in tablet form. Unlike a Tablet PC, the Internet tablet does not have much computing power and its applications suite is limited. Also it cannot replace a general-purpose computer. The Internet tablets typically feature an MP3 and video player, a Web browser, a chat application and a picture viewer.

**4. Personal digital assistant (PDA):** It is a small, usually pocket-sized, computer with limited functionality. It is intended to supplement and synchronize with a desktop computer, giving access to contacts, address book, notes, E-Mail and other features.

**5. Ultramobile PC:** It is a full-featured, PDA-sized computer running a general-purpose operating system (OS).

**6. Smartphone:** It is a PDA with integrated cell phone functionality. Current Smartphones have a wide range of features and installable applications.

**7. Carputer:** It is a computing device installed in an automobile. It operates as a wireless computer, sound system, *global positioning system (GPS) and DVD player*. It also contains word processing software and is Bluetooth compatible.

**8. Fly Fusion Pentop computer:** *It is a computing device with the size and shape of a pen. It functions as a writing utensil, MP3 player, language translator, digital storage device and calculator.*

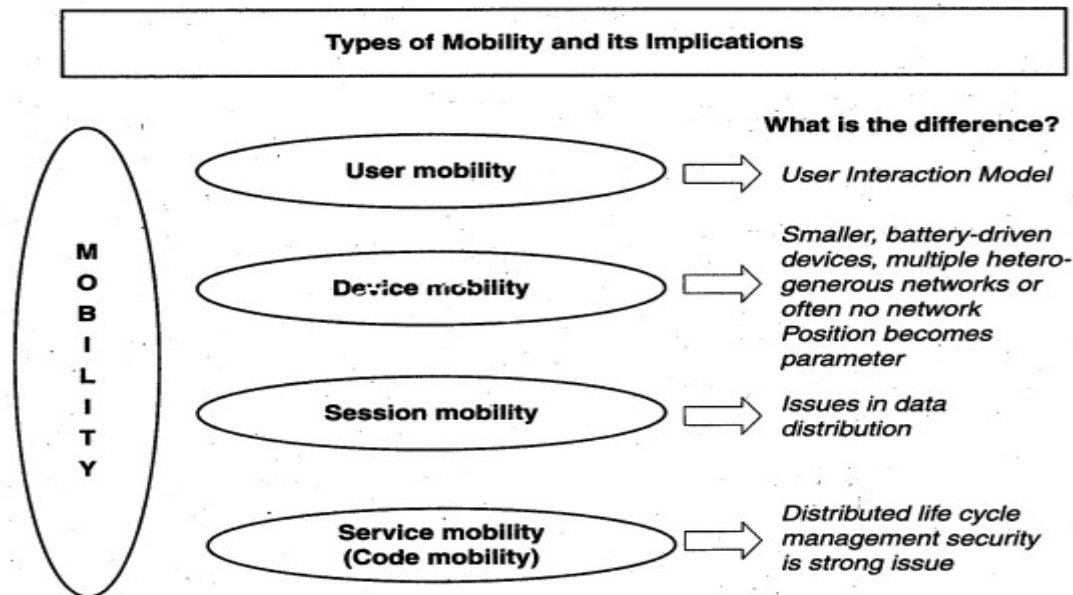
### **Wireless computing**

- Wireless refers to the method of transferring information between a computing device (such as a PDA) and a data source (such as an agency database server) without a physical connection.
- Not all wireless communication technologies are mobile. For example, lasers are used in wireless data transfer between buildings, but cannot be used in mobile communications at this time.
- Mobile simply describes a computing device that is not restricted to a desktop, that is, not tethered. As more personal devices find their way into the enterprise, corporations are realizing cybersecurity threats that come along with the benefits achieved with mobile solutions.
- Mobile computing does not necessarily require wireless communication. In fact, it may not require communication among devices at all.
- Thus, while “wireless” is a subset of “mobile,” in most cases, an application can be mobile without being wireless.
- Smart hand-helds are defined as hand-held or pocket-sized devices that connect to a wireless or cellular network, and can have software installed on them; this includes networked PDAs and Smartphones.

### **Trends in Mobility**

- Mobile computing is moving into a new era, third generation (3G), which promises greater variety in applications and have highly improved usability as well as speedier networking.

- “iPhone” from Apple and Google-led “Android” phones are the best examples of this trend and there are plenty of other developments that point in this direction.
- This smart mobile technology is rapidly gaining popularity and the attackers (hackers and crackers) are among its biggest fans.
- It is worth noting the trends in mobile computing; this will help readers to realize the seriousness of cybersecurity issues in the mobile computing domain.
- Figure 3.3 shows the different types of mobility and their implications.



**Figure: Mobility types and implications**

Popular types of attacks against 3G mobile networks are as follows:

**1. Malwares, viruses and worms:** Although many users are still in the transient process of switching from 2G, 2.5G to 3G, it is a growing need to educate the community people and provide awareness of such threats that exist while using mobile devices. Here are few examples of malware(s) specific to mobile devices:

- **Skull Trojan:** It targets Series 60 phones equipped with the Symbian mobile OS.
- **Cabir Worm:** It is the first dedicated mobile-phone worm; infects phones running on Symbian OS and scans other mobile devices to send a copy of itself to the first vulnerable phone it finds through Bluetooth Wireless technology. The worst thing about this worm is that the source code for the Cabir-H and Cabir-I viruses is available online.
- **Mosquito Trojan:** It affects the Series 60 Smart phones and is a cracked version of “Mosquitos” mobile phone game.
- **Brador Trojan:** It affects the Windows CE OS by creating a svchost.exe file in the Windows start-up folder which allows full control of the device. This executable file is conducive to traditional worm propagation vector such as E-Mail file attachments (refer to Appendix C).
- **Lasco Worm:** It was released first in 2005 to target PDAs and mobile phones running the Symbian OS. Lasco is based on Cabir’s source code and replicates over Bluetooth connection.

2. **Denial-of-service (DoS):** The main objective behind this attack is to make the system unavailable to the intended users. Virus attacks can be used to damage the system to make the system unavailable.
3. **Overbilling attack:** Overbilling involves an attacker hijacking a subscriber's IP address and then using it (i.e., the connection) to initiate downloads that are not "Free downloads" or simply use it for his/her own purposes. In either case, the legitimate user is charged for the activity which the user did not conduct.
4. **Spoofed policy development process (PDP):** These types of attacks exploit the vulnerabilities in the GTP [General Packet Radio Service (GPRS) Tunneling Protocol].
5. **Signaling-level attacks:** The Session Initiation Protocol (SIP) is a signaling protocol used in IP multimedia subsystem (IMS) networks to provide Voice Over Internet Protocol (VoIP) services. There are several vulnerabilities with SIP-based VoIP systems.

### Credit Card Frauds in Mobile and Wireless Computing Era

- These are new trends in cybercrime that are coming up with mobile computing – mobile commerce (M- Commerce) and mobile banking (M-Banking).
- Credit card frauds are now becoming commonplace given the ever- increasing power and the ever-reducing prices of the mobile hand-held devices, factors that result in easy availability of these gadgets to almost anyone.
- *Mobile credit card transactions* are now very common; new technologies combine low- cost mobile phone technologies with the capabilities of a point-of-sale (POS) terminal.
- Today belongs to "mobile computing," that is, *anywhere anytime computing*.
- The developments in wireless technology have fuelled this new mode of working for white collar workers.
- Wireless credit card processing is a very desirable system, because it allows businesses to process transactions from mobile locations quickly, efficiently and professionally.
- It is most often used by businesses that operate mainly in a mobile environment.
- Figure 3.4 shows the basic flow of transactions involved in purchases done using credit cards.

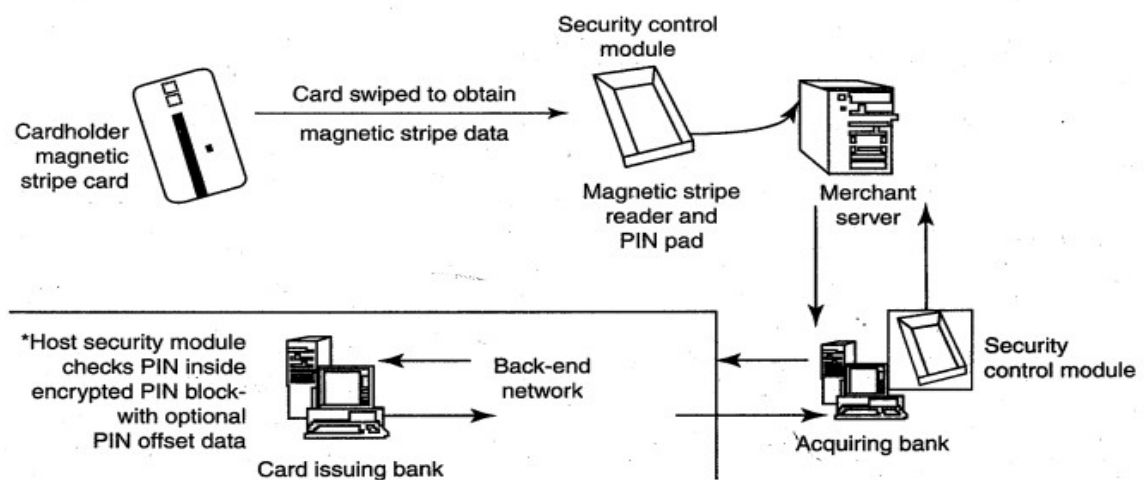
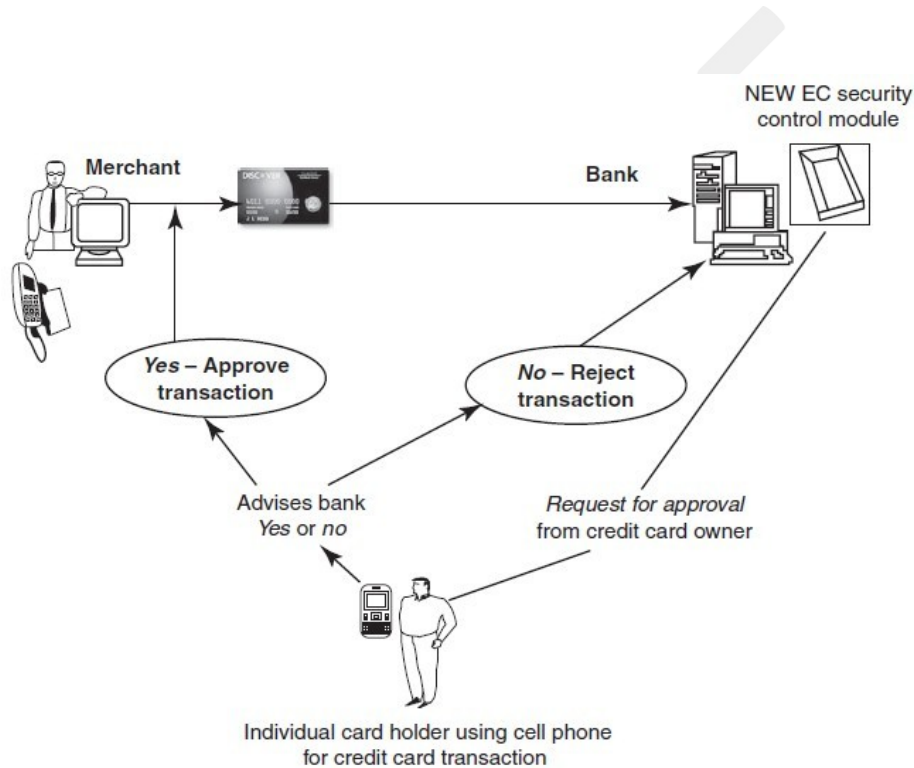


Figure : Online environment for credit card transactions



- Credit card companies, normally, do a good job of helping consumers resolve identity (ID) theft problems once they occur. But they could reduce ID fraud even more if they give consumers better tools to monitor their accounts and limit high-risk transactions
- Figure 3.5, the basic flow is as follows:
  1. Merchant sends a transaction to bank;
  2. The bank transmits the request to the authorized cardholder [*not* short message service (SMS)];
  3. The cardholder approves or rejects (password protected);
  4. The bank/merchant is notified;
  5. The credit card transaction is completed.



**Figure 3.5** Closed-loop environment for wireless (CLEW).  
 Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*. Wiley India.

**(Box 3.2). Tips to Prevent Credit Card Frauds**

- The current topic is about credit card frauds in mobile and wireless computing era, however, we would like to include these tips to prevent credit card frauds[8] caused due to individual ignorance about a few known facts.

**Do's**

1. Put your signature on the card immediately upon its receipt.
2. Make the photocopy of both the sides of your card and preserve it at a safe place to remember the card number, expiration date in case of loss of card.
3. Change the default *personal identification number* (PIN) received from the bank before doing any transaction.
4. Always carry the details about contact numbers of your bank in case of loss of your card.
5. Carry your cards in a separate pouch/card holder than your wallet.
6. Keep an eye on your card during the transaction, and ensure to get it back immediately.

7. Preserve all the receipts to compare with credit card invoice.
8. Reconcile your monthly invoice/statement with your receipts.
9. Report immediately any discrepancy observed in the monthly invoice/statement.
10. Destroy all the receipts after reconciling it with the monthly invoice/statement.
11. Inform your bank in advance, about any change in your contact details such as home address, cell phone number and E-Mail address.
12. Ensure the legitimacy of the website before providing any of your card details.
13. Report the loss of the card immediately in your bank and at the police station, if necessary.
<b>Dont's</b>
1. Store your card number and PINs in your cell.
2. Lend your cards to anyone.
3. Leave cards or transaction receipts lying around.
4. Sign a blank receipt (if the transaction details are not legible, ask for another receipt to ensure the amount instead of trusting the seller).
5. Write your card number/PIN on a postcard or the outside of an envelope.
6. Give out immediately your account number over the phone (unless you are calling to a company/ to your bank).
7. Destroy credit card receipts by simply dropping into garbage box/dustbin.

### 3.4.1 Types and Techniques of Credit Card Frauds

#### Traditional Techniques

- The traditional and the first type of credit card fraud is paper-based fraud – *application fraud*, wherein a criminal uses stolen or fake documents such as utility bills and bank statements that can build up useful personally Identifiable Information (PII) to open an account in someone else's name.
- Application fraud can be divided into
  1. **ID theft:** Where an individual pretends to be someone else
  2. **Financial fraud:** Where an individual gives false information about his or her financial status to acquire credit. Illegal use of lost and stolen cards is another form of traditional technique. Stealing a credit card is either by pickpocket or from postal service before it reaches its final destination.

#### Modern Techniques

- Skimming is where the information held on either the magnetic strip on the back of the credit card or the data stored on the smart chip are copied from one card to another.
- Site cloning and false merchant sites on the Internet are becoming a popular method of fraud and to direct the users to such bogus/fake sites is called Phishing.
- Such sites are designed to get people to hand over their credit card details without realizing that they have been directed to a fake weblink /website (i.e., they have been scammed).
- 1. **Triangulation:** It is another method of credit card fraud and works in the fashion as explained further.
  - The criminal offers the goods with heavy discounted rates through a website designed and hosted by him, which appears to be legitimate merchandise website.
  - The customer registers on this website with his/her name, address, shipping address and valid credit card details.
  - The criminal orders the goods from a legitimate website with the help of stolen credit card

details and supply shipping address that have been provided by the customer while registering on the criminal's website.

- The goods are shipped to the customer and the transaction gets completed.
- The criminal keeps on purchasing other goods using fraudulent credit card details of different customers till the criminal closes existing website and starts a new one.

**2. Credit card generators:** It is another modern technique – computer emulation software – that creates valid credit card numbers and expiry dates. The criminals highly rely on these generators to create valid credit cards. These are available for free download on the Internet.

---

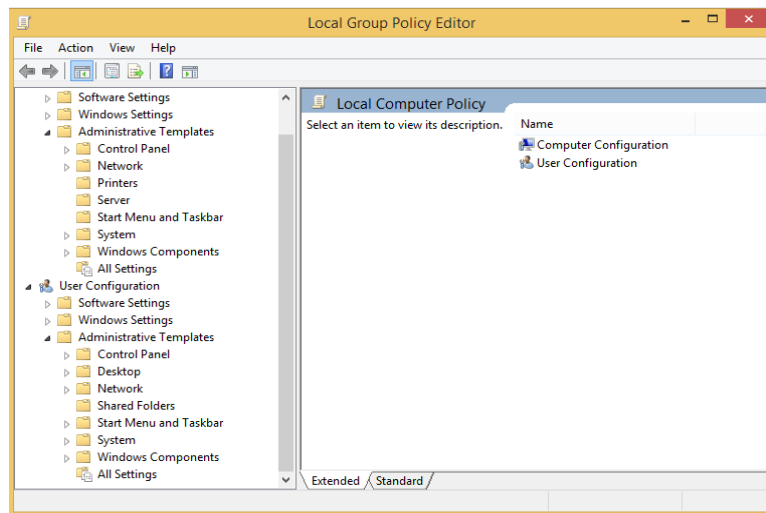
### **Security Challenges Posed by Mobile Devices**

- Mobility brings two main challenges to cybersecurity:
  - **first**, on the hand-held devices, information is being taken outside the physically controlled environment and
  - **second** remote access back to the protected environment is being granted.
- Perceptions of the organizations to these cybersecurity challenges are important in devising appropriate security operating procedure.
- As the number of mobile device users increases, two challenges are presented:
  1. at the device level called “microchallenges” and
  2. at the organizational level called “macrochallenges.”
- Some well-known technical challenges in mobile security are: *managing the registry settings and configurations, authentication service security, cryptography security, Lightweight Directory Access Protocol (LDAP) security, remote access server (RAS ) security, media player control security, networking application program interface (API ) security, etc.*

---

### **Registry Settings for Mobile Devices**

- Let us understand the issue of registry settings on mobile devices through an example:
  - Microsoft ActiveSync is meant for synchronization with Windows-powered personal computers (PCs) and Microsoft Outlook.
  - **ActiveSync** acts as the gateway between Windows-powered PC and Windows mobile-powered device, enabling the transfer of applications such as Outlook information, Microsoft Office documents, pictures, music, videos and applications from a user's desktop to his/her device.
  - In addition to synchronizing with a PC, ActiveSync can synchronize directly with the Microsoft exchange server so that the users can keep their E-Mails, calendar, notes and contacts updated wirelessly when they are away from their PCs.
  - In this context, **registry setting becomes an important issue given the ease with which various applications allow a free flow of information.**
- Thus, establishing trusted groups through appropriate registry settings becomes crucial. One of the most prevalent areas where this attention to security is applicable is within “group policy.” Group policy is one of the core operations that are performed by Windows Active Directory. (Run command box, type GPEDIT.MSC command to initiate the Local **Group Policy** Editor)

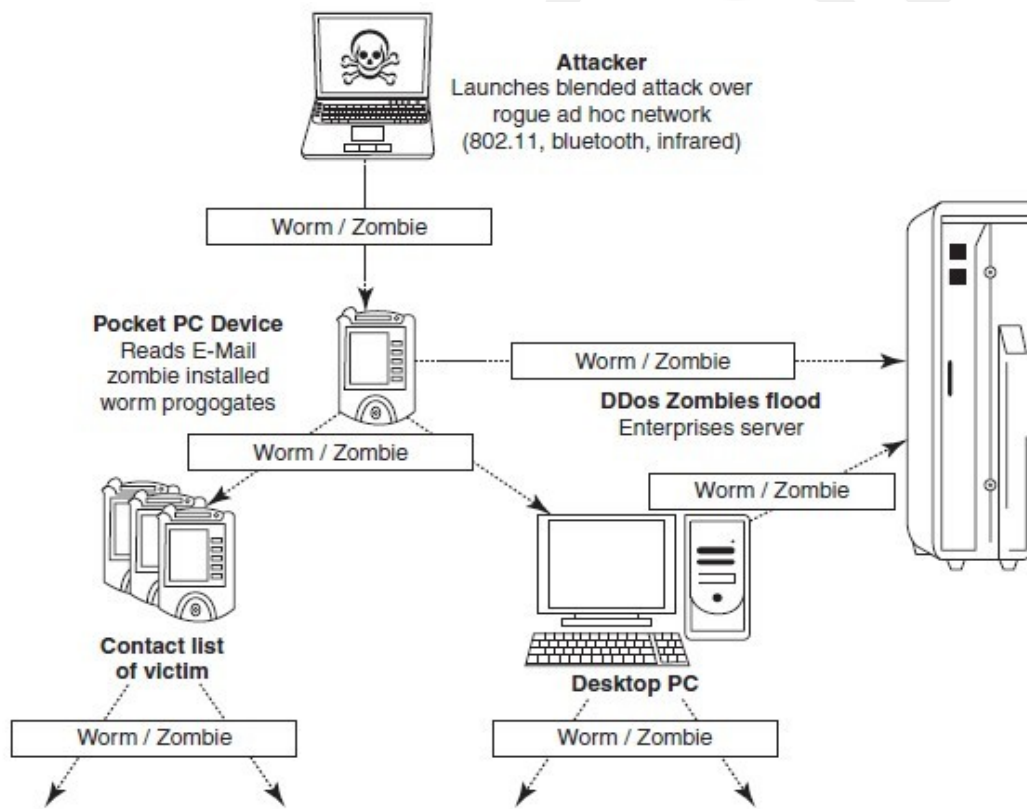


- There is one more dimension to mobile device security: new mobile applications are constantly being provided to help protect against *Spyware*, *viruses*, *worms*, *malware* and other Malicious Codes that run through the networks and the Internet.
- The mobile security issues on a Windows platform is that the baseline security is not configured properly.
- When you get a computer installed or use a mobile device for the first time, it may not be 100% secure. Even if users go through every *Control Panel setting* and *group policy* option, they may not get the computer to the desired baseline security.
- For example, the only way to get a Windows computer to a security level that will be near bulletproof is to make additional *registry* changes that are not exposed through any interface.
- There are many ways to complete these registry changes on every computer, but some are certainly more efficient than others.
- Naïve (Innocent) users may think that for solving the problem of mobile device security there are not many registry settings to tackle.
- However, the reality is far different! The reality of the overall problem becomes prevalent when you start researching and investigating the abundance of “registry hacks” that are discussed in Microsoft Knowledge Base articles.
- Figure 3.7 displays an illustration of how some tools allow users to browse to the desired registry value on their mobile devices.

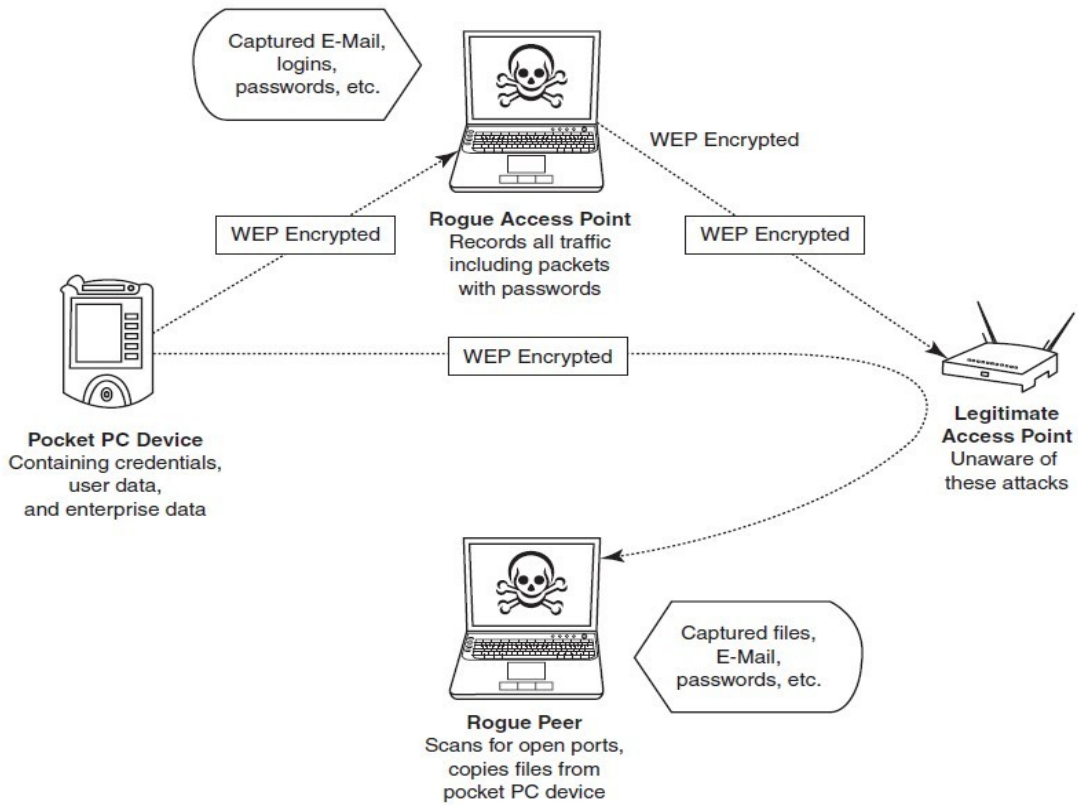


## Authentication Service Security

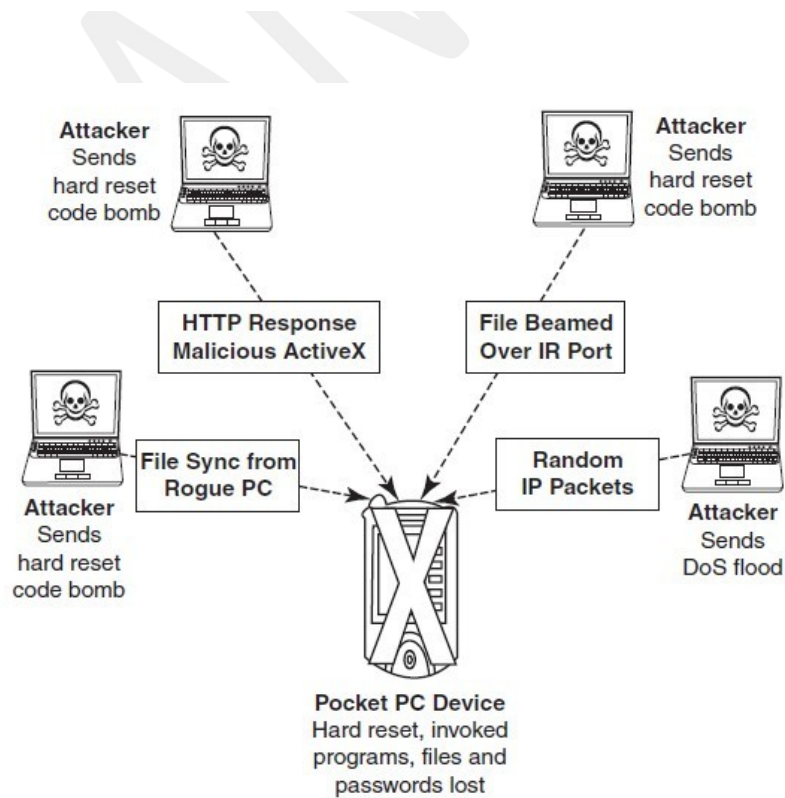
- There are two components of security in mobile computing: *security of devices* and *security in networks*.
- A secure network access involves mutual authentication between the device and the base stations or Web servers.
- This is to ensure that only authenticated devices can be connected to the network for obtaining the requested services.
- No Malicious Code can impersonate (imitate) the service provider to trick the device into doing something it does not mean to. Thus, the networks also play a crucial role in security of mobile devices.
- Some eminent kinds of attacks to which mobile devices are subjected to are: *push attacks*, *pull attacks* and *crash attacks* (see Figs. 3.8–3.10).
- Authentication services security is important given the typical attacks on mobile devices through wireless networks: *DoS attacks*, *traffic analysis*, *eavesdropping*, *man-in-the-middle attacks* and *session hijacking*.



**Figure 3.8** Push attack on mobile devices. DDoS implies distributed denial-of-service attack.  
Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.



**Figure 3.9** Pull attack on mobile devices.  
 Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.



**Figure 3.10** Crash attack on mobile devices. DoS – Denial-of-service attack.  
 Source: Nina Godbole (2009), *Information Systems Security: Security Management, Metrics, Frameworks and Best Practices*, Wiley India.

### Cryptographic Security for Mobile Devices

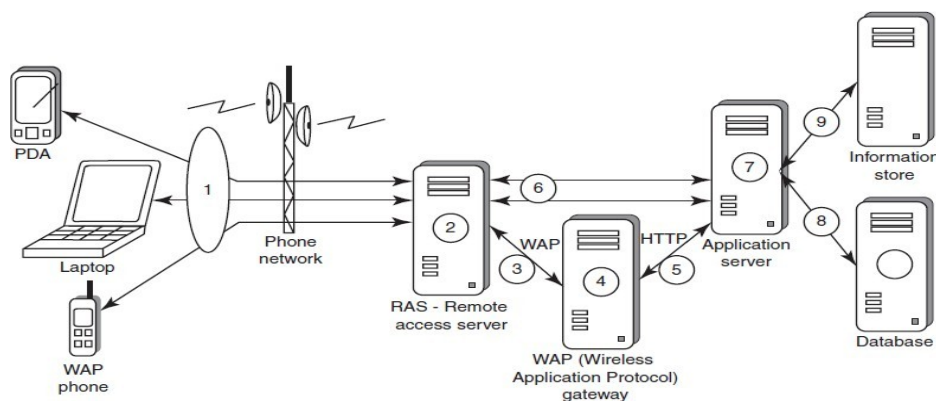
- **Cryptographically Generated Addresses (CGA)** is Internet Protocol version 6 (IPv6) that addresses up to 64 address bits that are generated by hashing owner's public-key address.
- The address the owner uses is the corresponding private key to assert address ownership and to sign messages sent from the address without a **public-key infrastructure (PKI)** or other security infrastructure.
- Deployment of **PKI** provides many benefits for users to secure their financial transactions initiated from mobile devices.
- CGA-based authentication can be used to protect IP-layer signaling protocols including neighbor discovery (as in *context-aware mobile computing applications*) and mobility protocols.
- It can also be used for key exchange in opportunistic Internet Protocol Security (IPSec). Palms (devices that can be held in one's palm) are one of the most common hand-held devices used in mobile computing.
- *Cryptographic security controls* are deployed on these devices.
- For example, the **Cryptographic Provider Manager (CPM)** in Palm OS5 is a system- wide suite of cryptographic services for securing data and resources on a palm-powered device.
- The CPM extends encryption services to any application written to take advantage of these capabilities, allowing the encryption of only selected data or of all data and resources on the device.

### LDAP (Lightweight Directory Access Protocol) Security for Hand-Held Mobile Computing Devices

- LDAP is a software protocol for enabling anyone to locate individuals, organizations and other resources such as files and devices on the network (i.e., on the public Internet or on the organizations's Intranet).
- In a network, a directory tells you where an entity is located in the network.
- LDAP is a light weight (smaller **Attacker** Launches blended attack over rogue ad hoc network (802.11, bluetooth, infrared) amount of code) version of **Directory Access Protocol (DAP)** because it does not include security features in its initial version.

### RAS (Remote Access Server) Security for Mobile Devices

- RAS (Remote Access Server) is an important consideration for protecting the business- sensitive data that may reside on the employees' mobile devices.
- In terms of cybersecurity, mobile devices are sensitive. Figure 3.11 : organization's sensitive data can happen through mobile hand-held devices carried by employees.





- In addition to being vulnerable to unauthorized access on their own, mobile devices also provide a route into the systems with which they connect.
- By using a mobile device to appear as a registered user (*impersonating* or *masquerading*) to these systems, a would-be cracker is then able to steal data or compromise corporate systems in other ways.
- Another threat comes from the practice of *port scanning*.
- First, attackers use a domain name system (DNS) server to locate the *IP address* of a connected computer. A *domain* is a collection of sites that are related in some sense.
- Second, they scan the ports on this known IP address, working their way through its Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) stack to see what communication ports are unprotected by firewalls.
- For instance, *File Transfer Protocol* (FTP) transmissions are typically assigned to port 21.
- If this port is left unprotected, it can be misused by the attackers (see Box 3.5).
- Protecting against port scanning requires software that can trap unauthorized incoming data packets and prevent a mobile device from revealing its existence and ID.
- A *personal firewall* on a pocket PC or Smartphone device can be an effective protective screen against this form of attack for the users connecting through a direct Internet or RAS connection.

### **Media Player Control Security**

- Various leading software development organizations have been warning the users about the potential security attacks on their mobile devices through the “music gateways.”
- There are many examples to show how a media player can turn out to be a source of threat to information held on mobile devices.
- For example, in the year 2002, Microsoft Corporation warned about this.
- According to this news item, Microsoft had warned people that a series of flaws in its Windows Media Player could allow a malicious hacker to hijack people’s computer systems and perform a variety of actions.
- According to this warning from Microsoft, in the most severe exploit of a flaw, a hacker could take over a computer system and perform any task the computer’s owner is allowed to do, such as opening files or accessing certain parts of a network.

### **Networking API Security for Mobile Computing Applications**

- With the advent of electronic commerce (E-Commerce) and its further off -shoot into *M-Commerce*, online payments are becoming a common phenomenon with the *payment gateways* accessed remotely and possibly wirelessly.
- Furthermore, with the advent of *Web services* and their use in mobile computing applications, the API becomes an important consideration.
- Already, there are organizations announcing the development of various APIs to enable software and hardware developers to write single applications
- Most of these developments are targeted specifically at securing a range of embedded and consumer products, including those running OSs such as Linux, Symbian, Microsoft Windows CE and Microsoft Windows Mobile (the last three are the most commonly used OSs for mobile devices).
- Technological developments such as these provide the ability to significantly improve cybersecurity of a wide range of consumer as well as mobile devices. Providing a common software framework, APIs will become an important enabler of new and higher value services.



## Attacks on Mobile/Cell Phones

### Mobile Phone Theft

- Mobile phones have become an integral part of everybody's life and the mobile phone has transformed from being a luxury to a bare necessity.
- Theft of mobile phones has risen dramatically over the past few years.
- Since huge section of working population in India use public transport, major locations where theft occurs are bus stops, railway stations and traffic signals.
- Many Insurance Companies have stopped offering Mobile Theft Insurance due to a large number of false claims.
- When anyone loses his/her mobile phone, more than anything "Contact List" and "Personally Identifiable Information (PII)", that really matter, are lost
- One might have just thought that his/her cell phone is much safer than a PC that is very often attacked by viruses; however, criminals made this thought as false statement.
- After PC, the criminals' (i.e., attackers') new playground has been cell phones, reason being the increasing usage of cell phones and availability of Internet using cell phones.
- Another reason is increasing demand for Wi-Fi zones in the metropolitans and extensive usage of cell phones in the youths with lack of awareness/knowledge about the vulnerabilities of the technology.
- The following factors contribute for outbreaks on mobile devices:
  - 1. Enough target terminals:** Enough terminals or more devices to attack.
  - 2. Enough functionality:** The expanded functionality i.e. *office functionality and applications* also increases the probability of malware.
  - 3. Enough connectivity:** Smartphones offer multiple communication options, such as SMS, MMS, synchronization, Bluetooth, infrared (IR) and WLAN connections.

#### **Box 3.6 | Tips to Secure your Cell/Mobile Phone from being Stolen/Lost**

Ensure to note the following details about your cell phone and preserve it in a safe place:

- 1.** Your phone number;
- 2.** the make and model;
- 3.** color and appearance details;
- 4.** PIN and/or security lock code;
- 5.** IMEI number.

#### **The International Mobile Equipment Identity (IMEI)**

- It is a number unique to every GSM, WCDMA and iDEN cell phone. It is a 15-digit number and can be obtained by entering \*#06# from the keypad.
  - The IMEI number is used by the GSM network to identify valid devices and therefore can be used to stop a stolen phone from accessing the network in that country.
  - For example, if a mobile phone is stolen, the owner can call his or her service provider and instruct them to "lock" the phone using its IMEI number.
  - This will help to stop the usage of phone in that country, even if a SIM is changed.
  - Visit the weblink <http://www.numberingplans.com/?page=analysis&sub=imeinr> to check all information about your cell phone such as manufacturer, model type and country of approval of a handset.
- Following are few antitheft software(s) available in the market:
    - 1. GadgetTrak:** <http://www.gadgettrak.com/products/mobile/>
    - 2. Back2u:** <http://www.bak2u.com/phonebakmobilephone.php>
    - 3. Wavesecure:** <https://www.wavesecure.com/>
    - 4. F-Secure:** <http://www.f-secure.com/>

## Mobile Viruses

- A mobile virus is similar to a computer virus that targets mobile phone data or applications/software installed in it.
- Virus attacks on mobile devices are no longer an exception or proof-of-concept nowadays.
- In total, 40 mobile virus families and more than 300(+) mobile viruses have been identified.
- First mobile virus was identified in 2004 and it was the beginning to understand that mobile devices can act as vectors to enter the computer network.
- Mobile viruses get spread through two dominant communication protocols – Bluetooth and MMS.
- Bluetooth virus can easily spread within a distance of 10–30 m, through Bluetooth- activated phones
- MMS virus can send a copy of itself to all mobile users whose numbers are available in the infected mobile phone’s address book.
- *How to Protect from Mobile Malwares Attacks*

Following are some tips to protect mobile from mobile malware attacks:

1. Download or accept programs and content (including ring tones, games, video clips and photos) only from a trusted source.
2. If a mobile is equipped with Bluetooth, turn it OFF or set it to non-discoverable mode when it is not in use and/or not required to use.
3. If a mobile is equipped with beam (i.e., IR), allow it to receive incoming beams, only from the trusted source.
4. Download and install antivirus software for mobile devices.

## **Mishing**

- *Mishing* is a combination of mobile and Phishing.
- Mishing attacks are attempted using mobile phone technology.
- M-Commerce is fast becoming a part of everyday life. If you use your mobile phone for purchasing goods/services and for banking, you could be more vulnerable to a Mishing scam.
- A typical Mishing attacker uses call termed as *Vishing* or message (SMS) known as *Smishing*.
- Attacker will pretend to be an employee from your bank or another organization and will claim a need for your personal details.
- Attackers are very creative and they would try to convince you with different reasons why they need this information from you.

## **Vishing**

- Vishing is the criminal practice of using social engineering over the telephone system, most often using features facilitated by VoIP, to gain access to personal and financial information from the public for the purpose of financial reward.
- The term is a combination of V – voice and Phishing.
- Vishing is usually used to steal credit card numbers or other related data used in ID theft schemes from individuals.
- The most profitable uses of the information gained through a Vishing attack include:
  1. ID theft;
  2. purchasing luxury goods and services;
  3. transferring money/funds;
  4. monitoring the victims’ bank accounts;
  5. making applications for loans and credit cards.

### How Vishing Works

- The criminal can initiate a Vishing attack using a variety of methods, each of which depends upon information gathered by a criminal and criminal's will to reach a particular audience.

**1. Internet E-Mail: 2. Mobile text messaging:**

**3. Voicemail: 4. Direct phone call:**

Following are the steps detailing on how direct phone call works:

- The criminal gathers cell/mobile phone numbers located and steals mobile phone numbers after accessing cellular company.
- The criminal often uses a dialer to call phone numbers of people from a specific region, and that to from the gathered list of phone numbers.
- When the victim answers the call, an automated recorded message is played to alert the victim that his/her credit card has had fraudulent activity and/or his/her bank account has had unusual activity. The message instructs the victim to call one phone number immediately. The same phone number is often displayed in the spoofed caller ID, under the name of the financial company the criminal is pretending to represent.
- When the victim calls on the provided number, he/she is given automated instructions to enter his/her credit card number or bank account details with the help of phone keypad.
- Once the victim enters these details, the criminal (i.e., visher) has the necessary information to make fraudulent use of the card or to access the account.
- Such calls are often used to gain additional details such as date of birth, credit card expiration date, etc.

Some of the **examples of vished** calls, when victim calls on the provided number after receiving phished E-Mail and/or after listening voicemail, are as follows:

**1. Automated message:** Thank you for calling (name of local bank). Your business is important to us. To help you reach the correct representative and answer your query fully, please press the appropriate number on your handset after listening to options.

- Press 1 if you need to check your banking details and live balance.
- Press 2 if you wish to transfer funds.
- Press 3 to unlock your online profile.
- Press 0 for any other query.

**2.** Regardless of what the victim enters (i.e., presses the key), the automated system prompts him to authenticate himself: "The security of each customer is important to us. To proceed further, we require that you authenticate your ID before proceeding. Please type your bank account number, followed by the pound key."

**3.** The victim enters his/her bank account number and hears the next prompt: "Thank you. Now please type your date of birth, followed by the pound key. For example 01 January 1950 press 01011950."

**4.** The caller enters his/her date of birth and again receives a prompt from the automated system: "Thank you. Now please type your PIN, followed by the pound key."

**5.** The caller enters his PIN and hears one last prompt from the system: "Thank you.

We will now transfer you to the appropriate representative." At this stage, the phone call gets disconnected, and the victim thinks there was something wrong with the telephone line; or visher may redirect the victim to the real customer service line, and the victim will not be able to know at all that his authentication was appropriated by the visher.

### How to Protect from Vishing Attacks

Following are some tips to protect oneself from Vishing attacks:

1. Be suspicious about all unknown callers.
2. Do not trust caller ID. It does not guarantee whether the call is really coming from that number, that is, from the individual and/or company – caller ID Spoofing is easy.
3. Be aware and ask questions, in case someone is asking for your personal or financial information.
4. Call them back. If someone is asking you for your personal or financial information, tell them that you will call them back immediately to verify if the company is legitimate or not. In case someone is calling from a bank and/or credit card company, call them back using a number displayed on invoice and/or displayed on website.
5. Report incidents: Report Vishing calls to the nearest cyberpolice cell with the number and name that appeared on the caller ID as well as the time of day and the information talked about or heard in a recorded message.

### Smishing

- Smishing is a criminal offense conducted by using social engineering techniques similar to Phishing.
- The name is derived from “SMS PhISHING.”
- SMS can be abused by using different methods and techniques other than information gathering under cybercrime.
- Smishing uses cell phone text messages to deliver a lure message to get the victim to reveal his/her PI.
- The popular technique to “hook” (method used to actually “capture” your information) the victim is either provide a phone number to force the victim to call or provide a website URL to force the victim to access the URL, wherein, the victim gets connected with bogus website (i.e., duplicate but fake site created by the criminal) and submits his/her PI.
- Smishing works in the similar pattern as Vishing.

### How to Protect from Smishing Attacks

Following are some tips to protect oneself from Smishing attacks:

1. Do not answer a text message that you have received asking for your PI. Even if the message seems to be received from your best friend, do not respond, because he/she may not be the one who has actually sent it.
2. Avoid calling any phone numbers, as mentioned in the received message, to cancel a membership and/or confirming a transaction which you have not initiated but mentioned in the message. **Always call on the numbers displayed on the invoice and/or appearing in the bank statements/passbook.**
3. **Never click on a hot link received through message on your Smartphone or PDA.** Hot links are links that you can click, which will take you directly to the Internet sites. Smishing messages may have hot links, wherein you click on the link and download Spyware to your phone without knowing. Once this software has been downloaded, criminals can easily steal any information that is available on your cell phone and have access to everything that you do on your cell phone.

## Hacking Bluetooth

- Bluetooth is an open wireless technology standard used for communication (i.e., exchanging data) over short distances (i.e., using short length radio waves) between fixed and/or mobile device.
- Bluetooth is a short-range wireless communication service/technology that uses the 2.4- GHz frequency range for its transmission/communication.
- The older standard – Bluetooth 1.0 has a maximum transfer speed of 1 Mbps (megabit per second) compared with 3 Mbps by Bluetooth 2.0.
- When Bluetooth is enabled on a device, it essentially broadcasts “I’m here, and I’m able to connect” to any other Bluetooth-based device within range.
- This makes Bluetooth use simple and straightforward, and it also makes easier to identify the target for attackers.
- The attacker installs special software [*Bluetooth hacking tools*] on a laptop and then installs a Bluetooth antenna.
- Whenever an attacker moves around public places, the software installed on laptop constantly scans the nearby surroundings of the hacker for active Bluetooth connections. Once the software tool used by the attacker finds and connects to a vulnerable Bluetooth- enabled cell phone, it can do things like download address book information, photos, calendars, SIM card details, make long-distance phone calls using the hacked device, bug phone calls and much more.

Table 3.1   Bluetooth hacking tools	
1.	<b>BlueScanner:</b> This tool enables to search for Bluetooth enable device and will try to extract as much information as possible for each newly discovered device after connecting it with the target.
2.	<b>BlueSniff:</b> This is a GUI-based utility for fi nding discoverable and hidden Bluetooth enabled devices.
3.	<b>BlueBugger:</b> The buggers exploit the vulnerability of the device and access the images, phonebook, messages and other personal information.
4.	<b>Bluesnarfer:</b> If a Bluetooth of a device is switched ON, then Bluesnarfing makes it possible to connect to the phone without alerting the owner and to gain access to restricted portions of the stored data.
5.	<b>BlueDiving:</b> Bluediving is testing Bluetooth penetration. It implements attacks like Bluebug and BlueSnarf.

*Bluejacking, Bluesnarfing, Bluebugging and Car Whisperer* are common attacks that have emerged as Bluetooth-specific security issues.

**1. Bluejacking:** It means *Bluetooth + Jacking* where Jacking is short name for *hijack* – act of taking over something. Bluejacking is sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or computers (within 10-m radius), Bluejacking is harmless, as bluejacked users generally do not understand what has happened and hence they may think that their phone is malfunctioning.

**2. Bluesnarfing:** It is the unauthorized access from a wireless device through a Bluetooth connection between cell phones, PDAs and computers. This enables the attacker to access a calendar, contact list, SMS and E-Mails as well as enable attackers to copy pictures and private videos.

**3. Bluebugging:** It allows attackers to remotely access a user's phone and use its features without user's attention.

**4. Car Whisperer:** It is a piece of software that allows attackers to send audio to and receive audio from a Bluetooth-enabled car stereo.

**Among the four above-mentioned attacks, Bluesnarfing is claimed to be much more serious than Bluejacking.**

These vulnerabilities are an inevitable result of technological innovation, and device manufacturers' continuously research and release firmware upgrades to address new challenges/problems as they arise.

"Bluetooth and Bluetooth Security" is a separate subject in itself. Readers may visit the following websites to explore more on this topic:

- <https://www.bluetooth.org/apps/content/>
- <http://www.bluetooth.com/English/Pages/default.aspx>
- <http://www.bluetoothhack.info/>

---

## **Mobile Devices: Security Implications for Organizations**

### **Managing Diversity and Proliferation of Hand-Held Devices**

- Cybersecurity is always a primary concern to Most organizations
- Most organizations fail to see the long-term significance of keeping track of who owns what kind of mobile devices.
- Mobile devices of employees should be registered to the organization.
- When an employee leaves, it is important to remove logical and physical access to organization networks.
- Thus, mobile devices that belong to the company should be returned to the IT department and, at the very least, should be deactivated and cleansed.

### **Unconventional/Stealth Storage Devices**

- Compact disks (CDs) and Universal Serial Bus (USB) drives (also called zip drive, memory sticks) used by employees are the key factors for cyber attacks.
- As the technology is advancing, the devices continue to decrease in size and emerge in new shapes and sizes –storage devices available nowadays are difficult to detect and have become a **prime challenge for organizational security**.
- It is advisable to prohibit the employees in using these devices.
- Not only can *viruses*, *worms* and *Trojans* get into the organization network, **but can also destroy valuable data in the organization network**.
- Organization has to have a policy in place to block these ports while issuing the asset to the employee.
- Employees can connect a USB/small digital camera/MP3 player to the USB port of any unattended computer and will be able to download confidential data or upload harmful viruses.
- As the malicious attack is launched from within the organization, firewalls and antivirus software are not alerted.
- Using "DeviceLock" software solution, one can have control over unauthorized access to plug and play devices (for more details, visit <http://www.devicelock.com/>).

- The features of the software allows system administrator to:
  1. Monitor which users or groups can access USB Ports, Wi-Fi and Bluetooth adapters, CD read-only memories (CD-ROMs) and other removable devices.
  2. Control the access to devices depending on the time of the day and day of the week.
  3. Create the white list of USB devices which allows you to authorize only specific devices that will not be locked regardless of any other settings.
  4. Set devices in read-only mode.
  5. Protect disks from accidental or intentional formatting.

### **Threats through Lost and Stolen Devices**

- This is a new emerging issue for cybersecurity.
- Often mobile hand-held devices are lost while people are on the move.
- Lost mobile devices are becoming even a larger security risk to corporations.
- A report based on a survey of London's 24,000 licensed cab drivers quotes that 2,900 laptops, 1,300 PDAs and over 62,000 mobile phones were left in London in cabs in the year 2001 over the last 6-month period.
- Today this figure (lost mobile devices) could be far larger given the greatly increased sales and usage of mobile devices.
- The cybersecurity threat under this scenario is scary; owing to a general lack of security in mobile devices, it is often not the value of the hand-held device that is important but rather the **content that, if lost or stolen, can put a company at a serious risk of sabotage, exploitation or damage to its professional integrity**, as most of the times the mobile hand-held devices are provided by the organization.
- Most of these lost devices have wireless access to a corporate network and have potentially very little security, making them a weak link and a major headache for security administrators.

### **Protecting Data on Lost Devices**

- There are two reasons why cybersecurity needs to protect the data when device is lost :
  1. data that are persistently stored on the device and
  2. always running applications.
- For protecting data, there are two precautions to prevent disclosure of the data stored on a mobile device:
  1. encrypting sensitive data and
  2. encrypting the entire file system.

## **Organizational Measures for Handling Mobile**

### **Encrypting Organizational Databases**

- Critical and sensitive data reside on databases and with the advances in technology, access to these data is possible through mobiles.
- Through encryption we can protect organization data.
- Two algorithms that are typically used to implement strong encryption of database files: **Rijndael** (pronounced rain-dahl or Rhine-doll), a **block encryption** algorithm, chosen as the new **Advanced Encryption Standard (AES)** for block ciphers by the National Institute of Standards and Technology (NIST).
- The other algorithm used to implement strong encryption of database files is the Multi-Dimensional Space Rotation (MDSR) algorithm developed by Casio.

- The term “strong encryption” is used here to describe these technologies in contrast to the simple encryption.
- *Strong encryption* means that it is much harder to break, but it also has a significant impact on performance.

### **Including Mobile Devices in Security Strategy**

- Organizational IT departments will have to take the accountability for cybersecurity threats that come through inappropriate access to organizational data from mobile- device–user employees.
- Encryption of corporate databases is not the end of everything.
- There are technologies available to properly secure mobile devices.
- For example, there are ways to make devices lock or destroy the lost data by sending the machine a special message.
- Also, some mobile devices have high-powered processors that will support 128-bit encryption.
- A few things that organization can use are:
  1. Implement strong asset management, virus checking, loss prevention and other controls for mobile systems that will prohibit unauthorized access and the entry of corrupted data.
  2. Investigate alternatives that allow a secure access to the company information through a firewall, such as mobile VPNs.
  3. Develop a system of more frequent and thorough security audits for mobile devices.
  4. Incorporate security awareness into your mobile training and support programs so that everyone understands just how important an issue security is within a company’s overall IT strategy.
  5. Notify the appropriate law-enforcement agency and change passwords. User accounts are closely monitored for any unusual activity for a period of time.

### **Organizational Security Policies and Measures in Mobile Computing Era**

#### **Importance of Security Policies relating to Mobile Computing Devices**

- Growth of mobile devices used makes the cybersecurity issue harder than what we would tend to think.
- People (especially, the youth) have grown so used to their mobiles that they are treating them like wallets!
- For example, people are storing more types of confidential information on mobile computing devices than their employers or they themselves know; they listen to music using their hand-held devices
- One should think about not to keep credit card and bank account numbers, passwords, confidential E-Mails and strategic information about organization.
- Imagine the business impact if mobile or laptop was lost or stolen, revealing sensitive customer data such as credit reports, social security numbers (SSNs) and contact information.

#### **Operating Guidelines for Implementing Mobile Device Security Policies**

- Through the following steps we can reduce the risk when mobile device lost or stolen
1. Determine whether the employees in the organization need to use mobile computing devices or not.
  2. Implement additional security technologies like strong encryption, device passwords and physical locks.



3. Standardize the mobile computing devices and the associated security tools being used with them.
4. Develop a specific framework for using mobile computing devices.
5. Maintain an inventory so that you know who is using what kinds of devices.
6. Establish patching procedures for software on mobile devices.
7. Label the devices and register them with a suitable service.
8. Establish procedures to disable remote access for any mobile.
9. Remove data from computing devices that are not in use
10. Provide education and awareness training to personnel using mobile devices.

### **Organizational Policies for the Use of Mobile Hand-Held Devices**

- There are many ways to handle the matter of creating policy for mobile devices.
- **One** way is creating a distinct mobile computing policy.
- **Another** way is including such devices under existing policy.
- 

### **Laptops**

- Laptops, like other mobile devices, enhance the business functions.
- Their mobile access to information anytime and anywhere, they also pose a large threat as they are portable.
- Wireless capability in these devices has also raised cybersecurity concerns when the information being transmitted over other, which makes it hard to detect.
- The thefts of laptops have always been a major issue, according to the cybersecurity industry and insurance company statistics.
- Cybercriminals are targeting laptops that are expensive, to enable them to fetch a quick profit in the black market.
- Most laptops contain personal and corporate information that could be sensitive.
- Such information can be misused if found by a malicious user.
- The following section provides some countermeasures against the theft of laptops, thereby avoiding cybersecurity exposures.

#### **3.12.1 Physical Security Countermeasures**

- Organizations are heavily dependent upon a mobile workforce with access to information, no matter where they travel.
- However, this mobility is putting organizations at risk of having a **data breach (Violation)** if a laptop containing sensitive information is lost or stolen.
- Hence, physical security is very important to protect the information on the employees' laptops.
- Physical security countermeasures are as follows.

**1. Cables and hardwired locks:** The most cost-efficient and ideal solution to safeguard any mobile device is securing with cables and locks, specially designed for laptops.

**2. Laptop safes:** Safes made of polycarbonate – the same material that is used in bulletproof windows, police riot shields and bank security screens – can be used to carry and safeguard the laptops

**3. Motion sensors and alarms:** Alarms and motion sensors are very efficient in securing laptops.

**4. Warning labels and stamps:** Warning labels containing tracking information and identification details can be fixed onto the laptop to deter aspiring thieves. These labels cannot be removed easily and are a low-cost solution to a laptop theft.

### 5. Other measures for Protecting laptops are as follows:

- keeping the laptop close to oneself wherever possible;
- carrying the laptop in a different and unobvious bag
- creating the awareness among the employees about the sensitive information contained in the laptop;
- making a copy of the purchase receipt of laptop
- installing encryption software to protect information stored on the laptop;
- using personal firewall software to block unwanted access and intrusion;
- updating the antivirus software regularly;
- tight office security using security guards and securing the laptop by locking it down in lockers when not in use;
- never leaving the laptop unattended in public places
- disabling IR ports and wireless cards when not in use.
- Choosing a secure OS
- Registering the laptop with the laptop manufacturer to track down the laptop in case of theft.
- Disabling unnecessary user accounts and renaming the administrator account.
- Backing up data on a regular basis.

A few logical access controls are as follows:

1. Protecting from malicious programs/attackers/social engineering.
2. Avoiding weak passwords/open access.
3. Monitoring application security and scanning for vulnerabilities.
4. Ensuring that unencrypted data/unprotected file systems do not pose threats.
5. Proper handling of removable drives/storage mediums/unnecessary ports.
6. Password protection through appropriate passwords rules and use of strong passwords.
7. Locking down unwanted ports/devices.
8. Regularly installing security patches and updates.
9. Installing antivirus software/firewalls/intrusion detection system (IDSs).
10. Encrypting critical file systems.
11. Other countermeasures:

#### **Box 3.13 | Spy Phone Software!!!**

Spy Phone software is installed on the mobile/cell phone of employees, if the employers wants to monitor phone usage. The Spy Phone software is completely hidden from the user, once it is installed and collects all the available data such as SMS messages, ingoing/outgoing call history, location tracking, GPRS usage and uploads the collected data to a remote server.

The employer can simply access the designated website hosted by Spy Phone vendor, and after entering his/her account details, he/she can have full access to all the data collected 24 hours a day, 7 days a week. The employer can access this website through the Internet; hence, he/she can keep an eye on their employees, regardless where he/she is in the world. The employer can read all SMS messages (both incoming and outgoing), know who they (employees) are calling or who is calling them and where they were when the call was received.

Following are few Spy Phone Software(s) available in the market:

1. **SpyPhonePlus:** <http://www.spyphoneplus.com/>
2. **FlexiSpy:** <http://www.flexispy.com/>
3. **TheSpyPhone:** <http://www.thespyphone.com/spyphone.html>
4. **Mobile Spy:** <http://www.mobile-spy.com/>

## Unit-4

# Cyber security: Organizational Implications

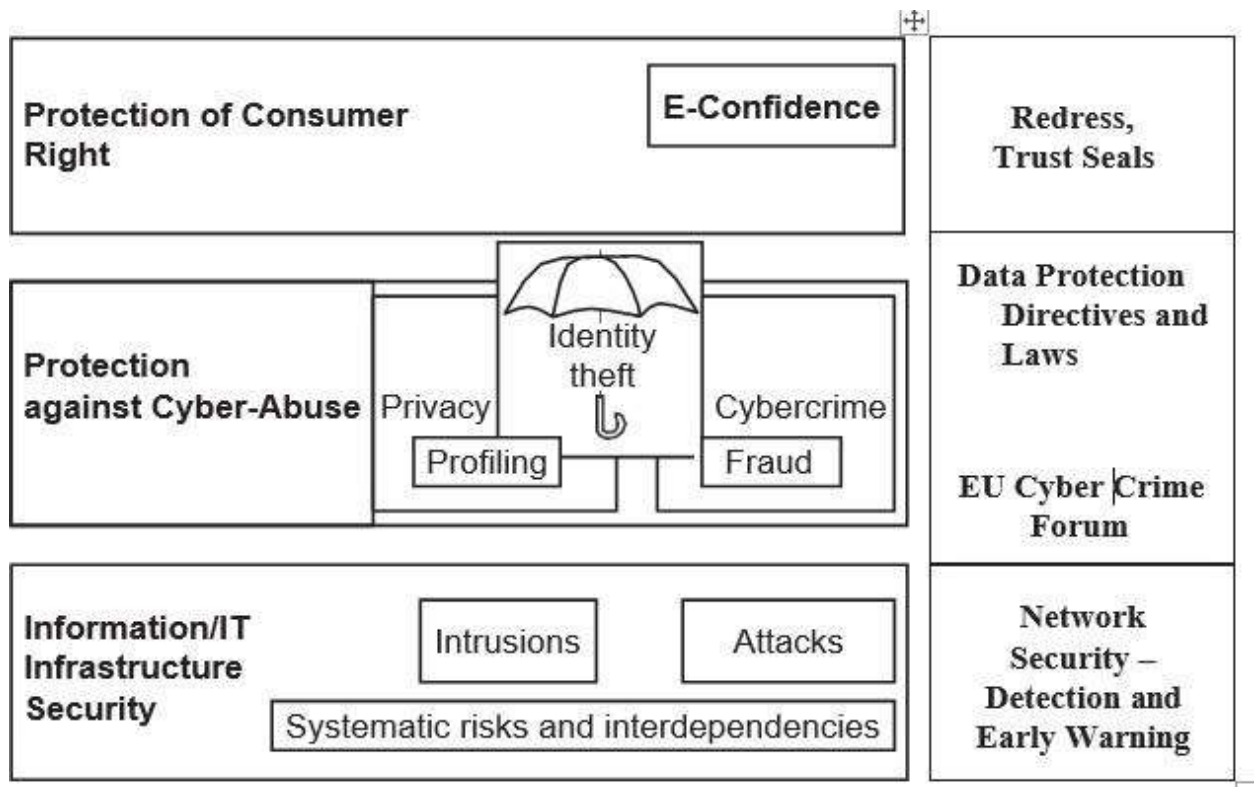
## Introduction

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.

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

To understand the relevant aspects of cyber-crimes in perspective, refer figure below



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

Author's experience in the industry as well as literature survey shows that such threats are large (as shown in figure below).

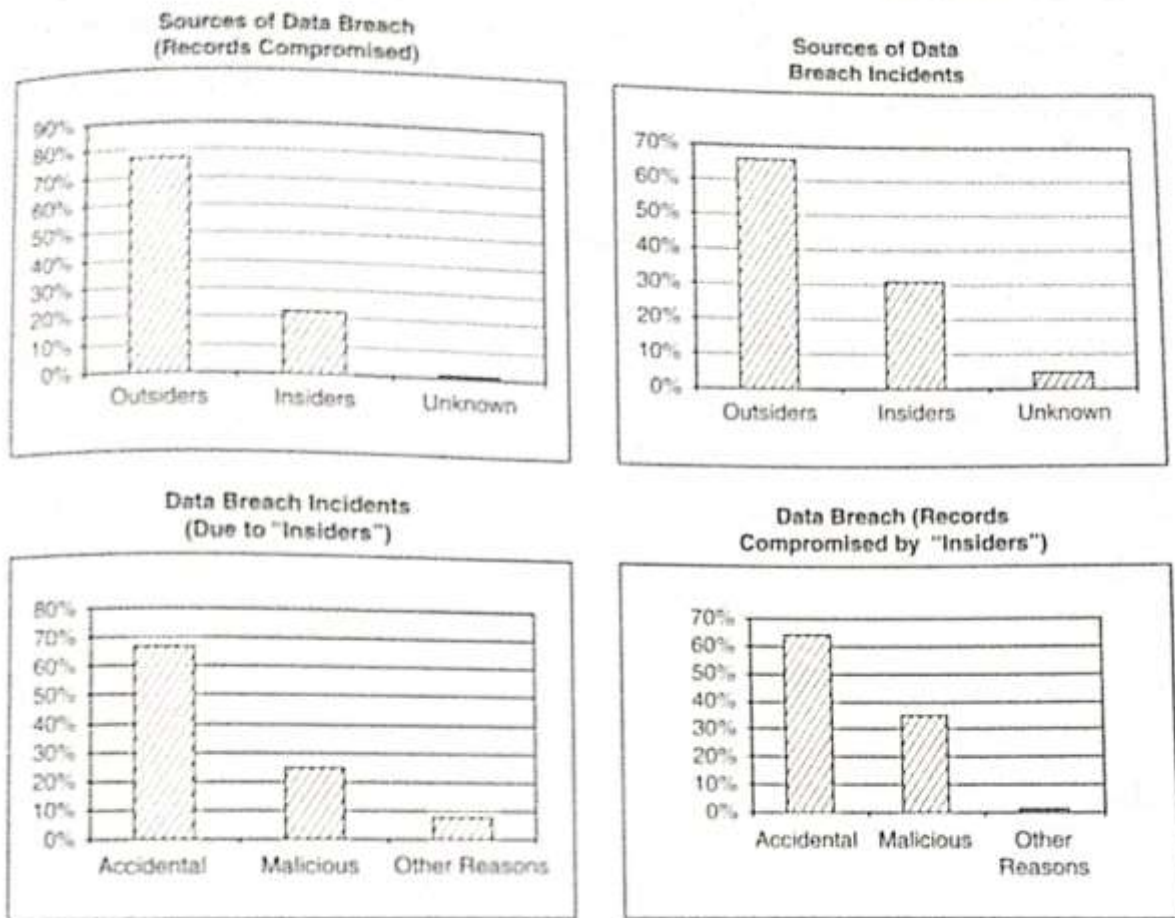


Figure 9.2 | Insider threat scenario (2000-2009).

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

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

Most information the organization collects about an individual is likely to come under “PI” category if it can be attributed to an individual. For an example, PI is an individual’s first name or first initial and last name in combination with any of the following data:

1. Social security number (SSN)/social insurance number.
2. Driver’s license number or identification card number.

3. Bank account number, credit or debit card number with personal identification number such as an access code, security codes or password that would permit access to an individual's financial account.
4. Home address or E-Mail address.
5. Medical or health information.

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

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

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

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

A case in point is the infamous “Heartland Payment System Fraud” that was uncovered in January 2010. This incident brings out the glaring point about seriousness of “insider attacks.

In this case, the concerned organization suffered a serious blow through nearly 100 million credit cards compromised from at least 650 financial services companies. When a card is used to make a purchase, the card information is transmitted through a payment network.

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

clients. Digital information within the magnetic stripe on the back of credit and debit cards was copied by keylogger.

## **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.

[http://en.wikipedia.org/wiki/Blue\\_Cross\\_Blue\\_Shield\\_Association](http://en.wikipedia.org/wiki/Blue_Cross_Blue_Shield_Association).

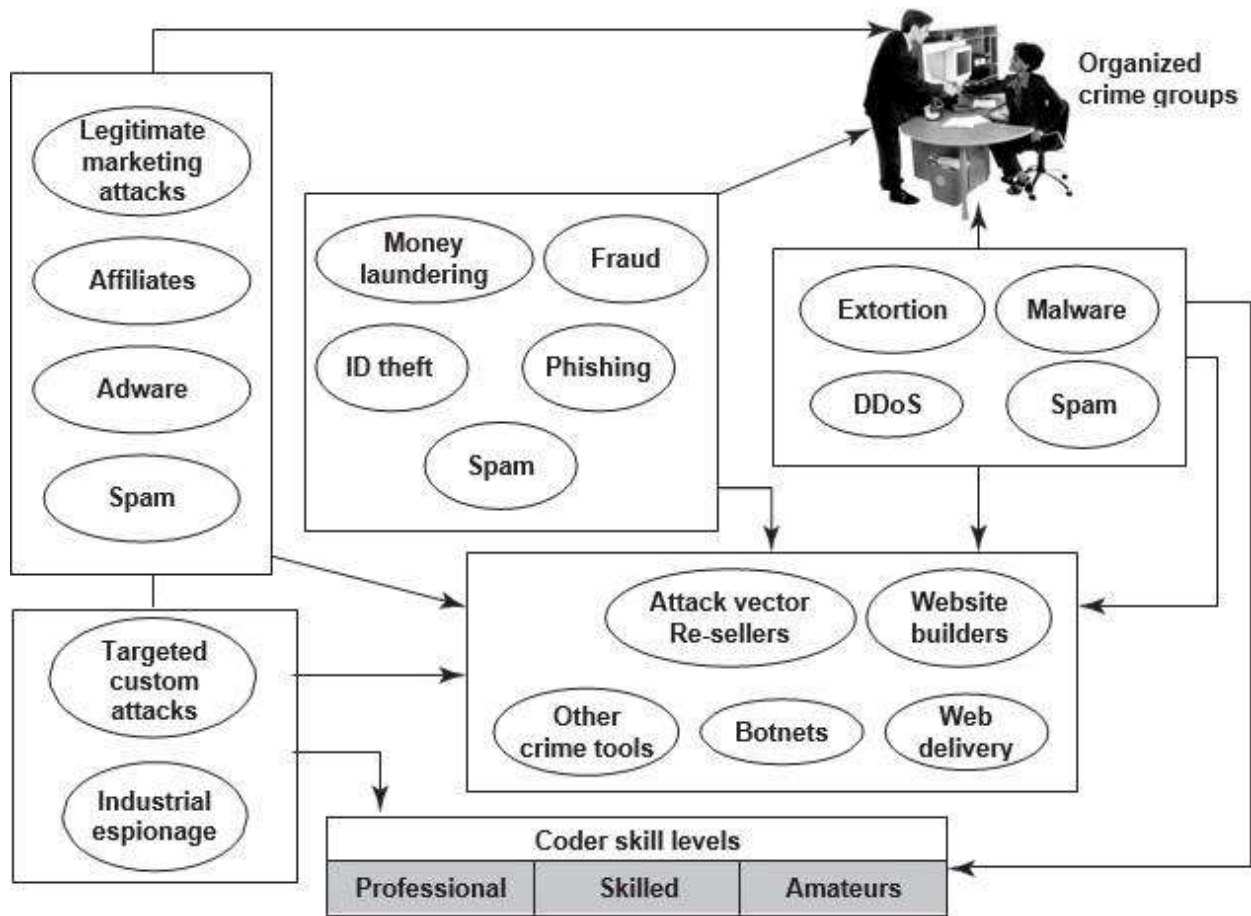
The hard drives containing 13 million audio files and 300,000 video files related to coordination of care and eligibility telephone calls from providers and members were reportedly stolen from a leased office.

Three hard drives (3.5"x10") were physically removed from server racks on computer inside data storage closet at a training center.

The two lessons to be learnt from this are:

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

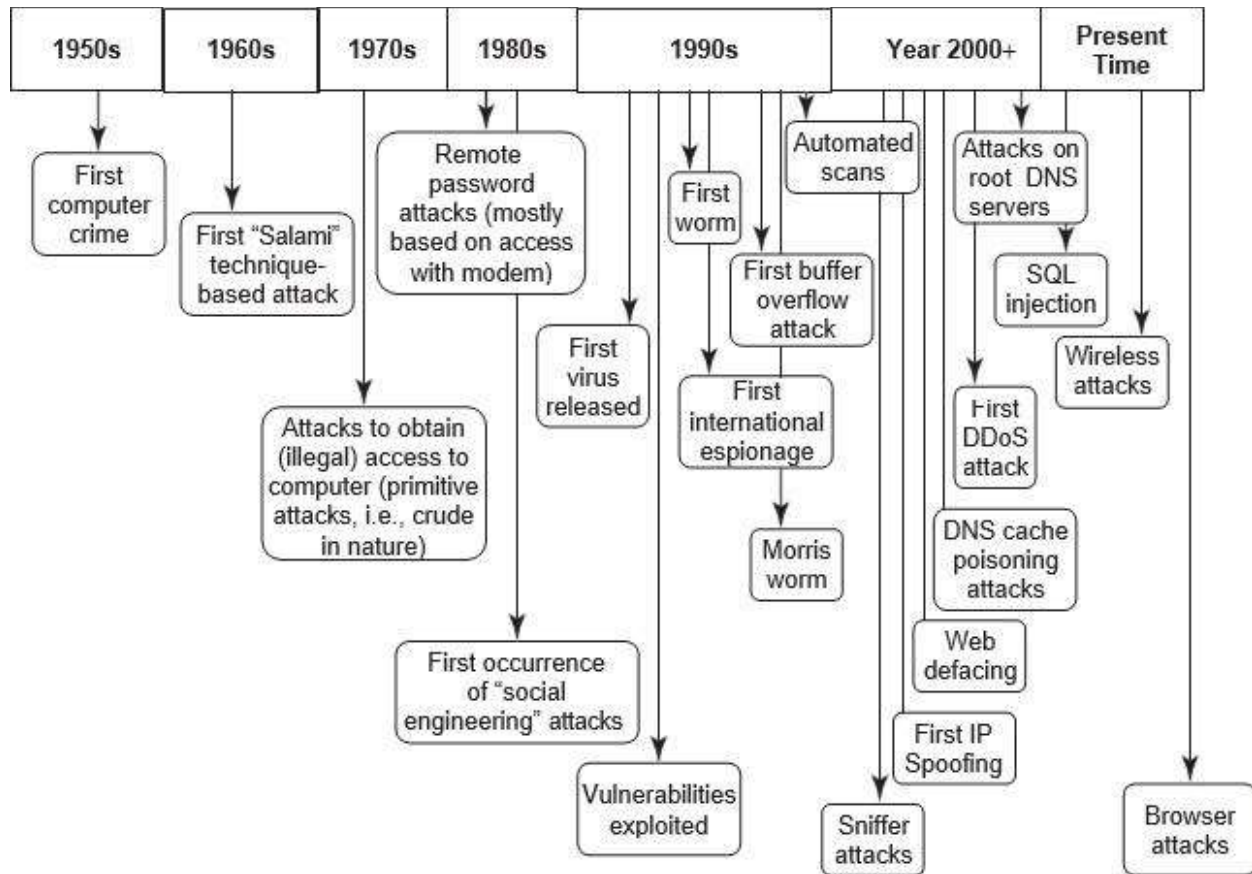
What makes matters worse is that the groups/agencies/entities connected with cybercrimes are all linked (Figure below)



**Fig: Cybercrimes – the flow and connections.**

There is certainly a paradigm shift in computing and work practices; with workforce mobility, virtual teams, social computing media, cloud computing services being offered, sharp rise is noticed in business process outsourcing (BPO) services, etc. to name a few.

Over a period of time, security threats to organizations have morphed from simple ones to very sophisticated one as shown in figure below



**Fig: Security threats – paradigm shift.**

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 cyber security 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.

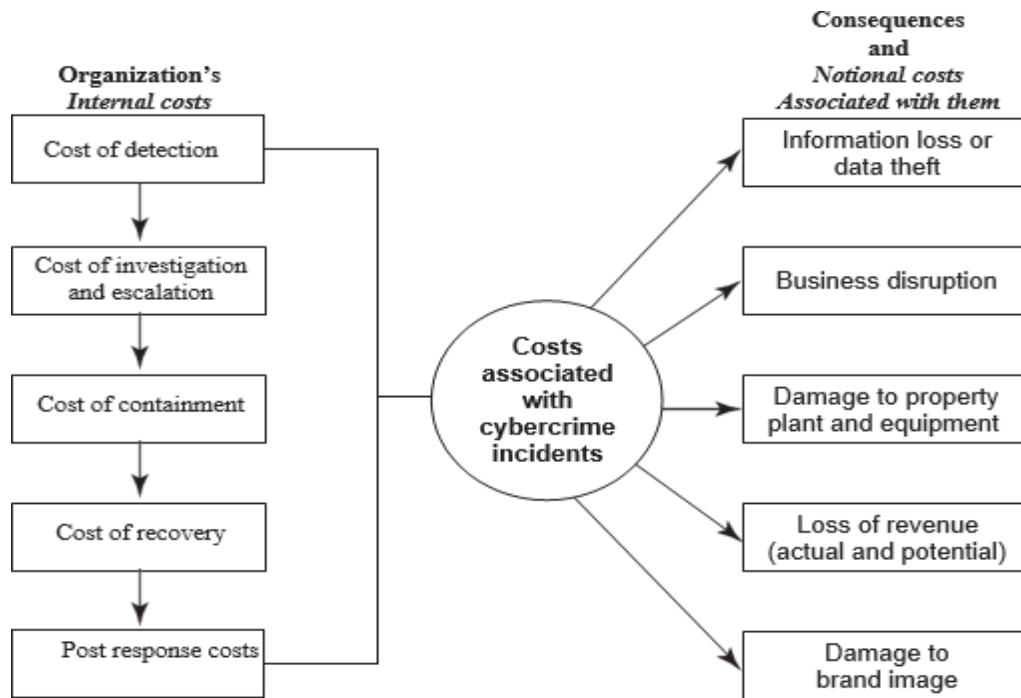


The key challenges from emerging new information threats to organizations are as follows:

- 1. Industrial espionage:** There are several tools available for web administrators to monitor and track the various pages and objects that are accessed on their website. For example, suppose your competitor's networks, using their firewalls and Intrusion Detection System (IDS) detect a large amount of traffic coming from your IP to their product page, then they may conclude that your organization is planning to come out with a similar product. This may make them take an anticipative action, in counter by launching a new promotion to thwart the impact of your new product campaign
- 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. There are websites that changes their online content depending on user's IP address or user's geographic location.
- 4. Cyber terrorism:** "Cyber terrorism" 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. (see Figure below)



**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. In this study, they found that the total annualized cost of cybercrime for the sampled organizations ranged from a low of US\$1 to US\$532 million.

With the growth in the use of internet these days the cyber crimes are also growing. Cyber theft of Intellectual Property (IP) is one of them. Cyber theft of IP means stealing of copyrights, trade secrets, patents etc., using internet and computers.

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

The internal costs typically involve *people costs, overhead costs and productivity losses*.

The internal costs, in order from largest to the lowest and that have been supported by the benchmark study mentioned:

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%)

The consequences of cybercrimes and their associated costs, mentioned

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%)

The benchmark study mentioned above revealed that the percentage of organizations impacted by various types of cybercrimes show the following distribution:

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

According to the benchmarks study mentioned above, when the data for “average days taken to resolve cyber attacks” was formulated according to the cyber attack categories, the following emerged as the picture

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

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

Again, there are lessons to learn:

- 1. Endpoint protection:** It is an often-ignored area but it is important. 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.

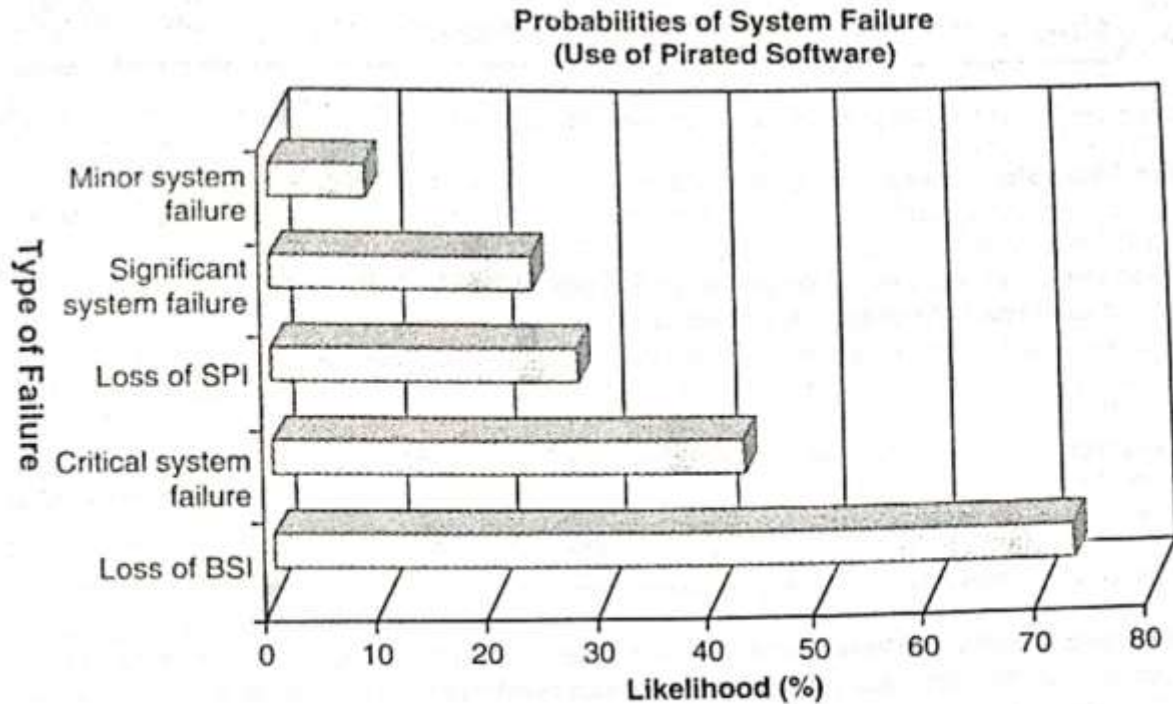
## **Organizational Implications of Software Piracy**

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.

Non genuine software can potentially disrupt smooth functioning of an organization's operations by adversely affecting the system security infrastructure (Figure Below)



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

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

Large number of companies as well as individuals has 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.

### Mobile Workforce – Category of “Remote Workers”

1. ***Tethered/remote worker***: This is considered to be an employee who generally remains at a single point of work, but is remote to the central company systems. This includes home workers, telecottagers, and in some cases, branch workers.
2. ***Roaming user***: This is either an employee who works in an environment (eg: ware housing, shop floor etc) or in multiple areas (eg. Meeting rooms)
3. ***Nomad***: This category covers employees requiring solutions in hotel rooms and other semitethered environments where modem use is still prevalent, along with the increasing use of multiple wireless technologies and devices.
4. ***Road warrior***: This is the ultimate mobile user, such as remote worker spends little time in the office; however, he/she requires regular access to data and collaborative functionality while on the move, in transit, or in hotels. This type includes the sales and field forces.

There is another way of classifying the workforce:

1. ***Office-based mobile workers***: These are the ones who spend most of their time in a company provided office, but they also sometimes work at home or in a third place.

2. *Non office based mobile workers:* These are the ones in the field, such as a salesperson, or workers between buildings on a corporate campus, such as IT professionals. They are more often at someone else's office than their own
3. *Home-based mobile workers:* These are the former telecommuter; this employee class spends most of the week working in a home office, but comes into the corporate workplace for meetings or collaborative work sessions.

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 etc.

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:

### **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.

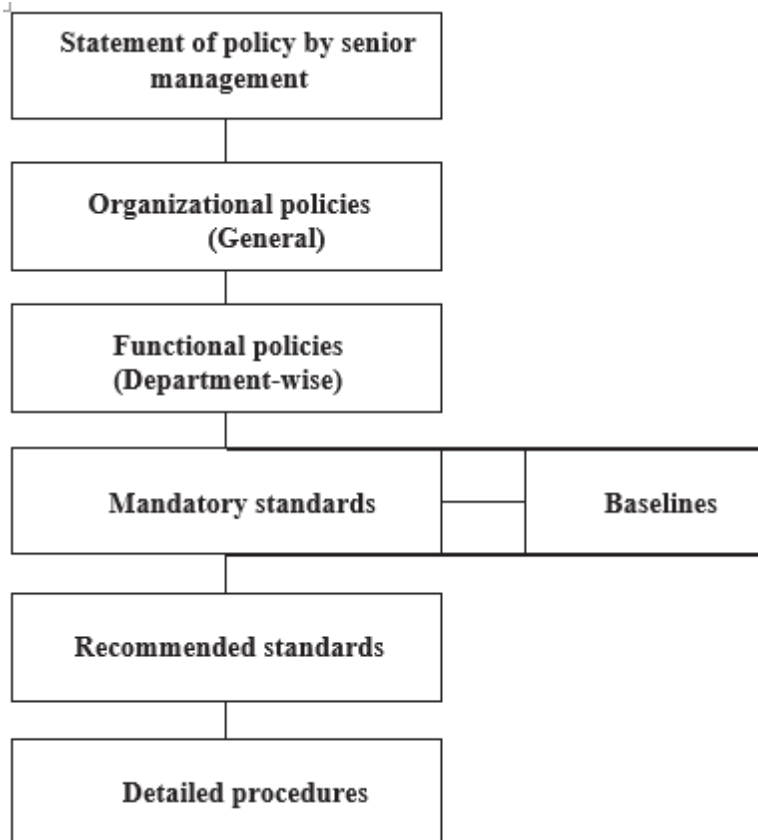
People seem to spend approximately 45-60 minutes each working day on personal web surfing at work.

Cookies stores the surfing activities.

### **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 cyber world! 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.

# 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.

## Social Media Marketing: Security Risks and Perils for Organizations

Social media marketing has become dominant in the industry.

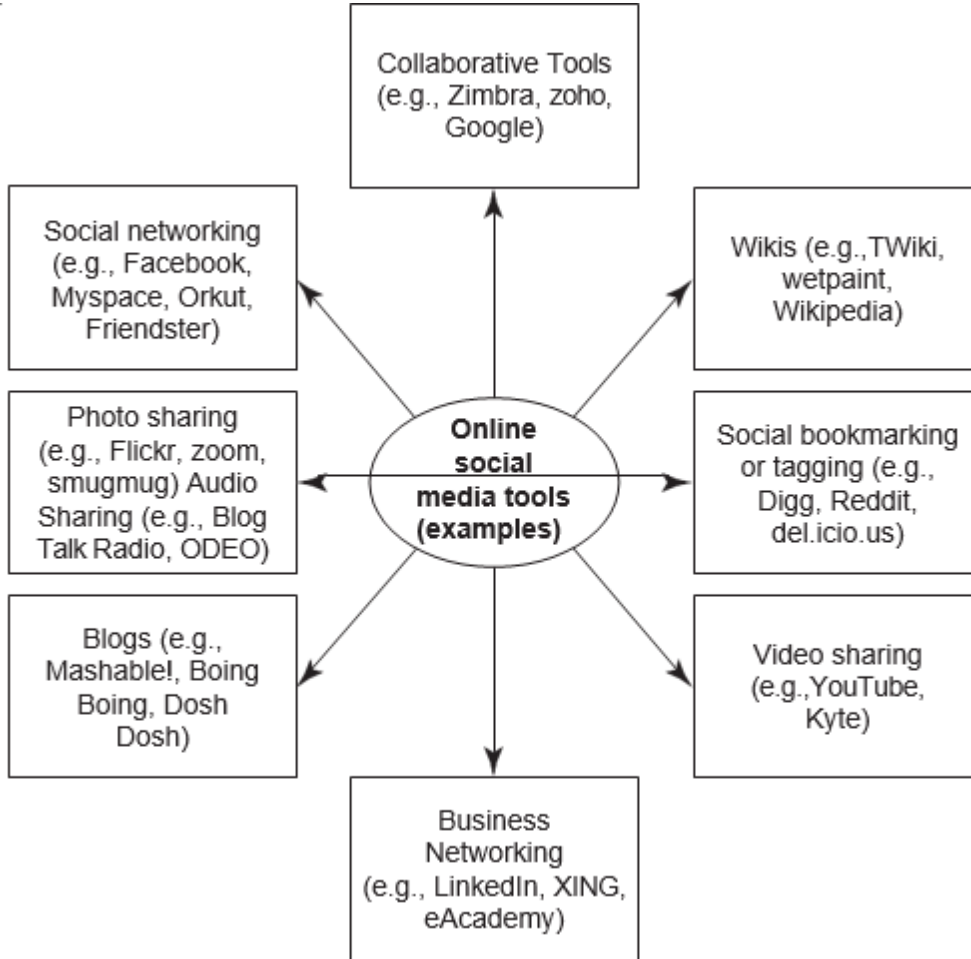
According to fall 2009 survey by marketing professionals, usage of social media sites by large business-to-business (B2B) organizations shows the following:

1. Face book 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.”

Figure below shows different types of social media tools



**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 as user 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 community of top executives from the Fortune 500.
3. Face book as the social group or social community tool is used to drive more traffic to Web sense website and increase awareness about Web sense.
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.

## **Best Practices with use of Social Media Marketing Tools**

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

Once the policy is created, employers should communicate it to employees and should enforce its implementation through continuous monitoring.

Increasing employee awareness is an ongoing activity. There is no go without it. This is because people can change their way of behaving in social networks only if they are aware of the security risks, sometimes they are genuinely not aware of those risks. Therefore, organizations need to educate their employees about their 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.

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

*Once you have social media usage policy in place, next steps are to establish firm processes based on that policy. 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. For example, administrators should ensure that the latest security updates are downloaded. Although it seems to be mundane and boring activity, it is crucial. Organizations must enable their IT administrators to identify network attacks in time or to avoid them altogether. IDS and firewalls play a crucial role here. Refer to Ref. #2, Books, Further Reading for a detail discussion on IDS and firewalls.*

Mere policies and procedures are of no use if you do not have the mechanism to maintain a strong controls posture. 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. Compliance requirements should also be taken into consideration. Policies should not be treated as a one-time activity. The important thing is to keep the policies up to date and adapt them to changing circumstances. Access management is addressed in Section 9.11.

Blocking the infected websites is another necessary activity. Recall the discussion about Trojan, viruses, worms, etc. in Chapter 2 – an action such as a person clicking on an infected website to download a Trojan can happen even when employees are taken through regular awareness training. Attrition in the organizations means that well-aware employees leave and new employees join! URL filters allow organizations to block access to known malware and Phishing websites (Phishing is discussed in Chapter 5). Access blocking can also be applied to any other suspicious site on the Internet. The filter function should be kept continuously up to date by maintaining so-called black- and white-listed websites.

Firewalls help to protect the organization (for more information refer to Ref. #2, Books, Further Reading). Using next-generation firewalls helps organizations keep their security technology up to date. Some firewalls provide a comprehensive analysis of all data traffic. Deep inspection of network traffic makes it possible to monitor the type of data traffic, the websites from which it is coming, to know the web browsing patterns and peer-to-peer applications to encrypted data traffic in SSL tunnel. (For Secure Socket Layer – SSL refer to Ref. #3, Books, Further Reading.) SSL is a process for inspection. The firewall decrypts the SSL data stream for inspection and encrypts it again before forwarding the data to the network. This results in effective protection of workstations and other endpoints, internal networks, hosts and servers against attacks within SSL tunnels.

Protection against vulnerability is possible by carefully planning vulnerability scanning and penetration testing (refer to Ref. #6, Books, Further Reading). Vulnerabilities present a huge challenge to any corporate network. In addition to the routine risks, organizations need to worry about the fact that attacks on vulnerabilities via the social web services are steadily increasing. An intrusion prevention system (IPS) serves as a protective barrier to the corporate network. An IPS automatically prevents attacks by worms, viruses or other

malware (refer to discussion in Chapter 2). Having identified an attack, the IPS immediately stops it and prevents it from spreading in the network. The IPS also enables patching of servers and services by securing servers under security threat, which will then be patched during the next maintenance window.

We mentioned about “need-based” access; organizations should define access to business applications that reside on corporate networks as well on the external sites. In Chapter 3, there is a discussion about careless use of mobile devices contributing to cybercrimes. There is a phenomenal rise in workforce mobility; mobile users, partners and distributors often need to access a corporate network while away from work place. Within this group, the use of social media can be monitored only on a very limited basis or not at all. This makes it even more important to assign the rights for defining all network access centrally, for example, using an SSL VPN portal – VPN is virtual private network, a tunnel within the Internet. At the same time, on the user level a strong authentication via single sign-on makes the administrator’s work easier. As a result, a single login makes it possible for users to access only the network areas and services for which they are authorized. Readers can refer to presentation and subsequent article on workforce mobility and challenges.<sup>[1]</sup>

Even the Intranets are not spared by cyberattackers. Therefore, securing the Intranets should also be included in the protection activities. The Intranet of every company contains highly sensitive information pertaining to the business areas involved (see Table 9.1). These areas need to be isolated from the rest of the

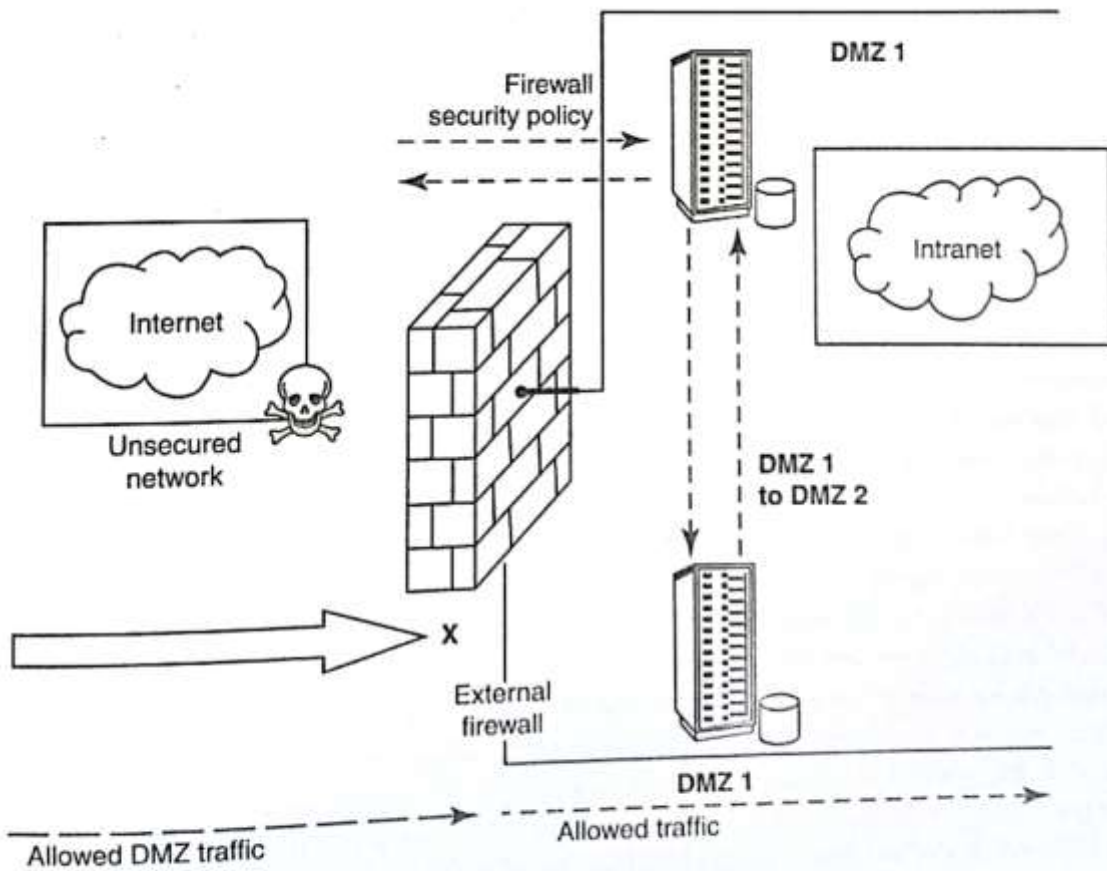


**Table 9.1** | Business area-wise information

<i>Business Area</i>	<i>Coverage</i>	<i>Typical Examples</i>	<i>Remarks</i>
<b>Business environment</b>	Business conditions external to the organization that can impact its business activities	<ol style="list-style-type: none"> <li>1. Rules and compliance set by regulatory agencies</li> <li>2. Issues created by Competitors</li> <li>3. Licensing authorities' requirements</li> </ol>	These may not be handled in a computerized manner inside a company data warehouse
<b>Customers and other affinity organizations</b>	People and organizations who acquire and/or use the company's products	<ol style="list-style-type: none"> <li>1. Prospects</li> <li>2. Customers</li> </ol>	Organizations use these mechanisms for capturing potential customers (prospects) and for distinguishing between parties who buy the product and those who use it
<b>Communications</b>	Messages and the media used to transmit them	<ol style="list-style-type: none"> <li>1. Advertisement campaigns</li> <li>2. Target audience</li> <li>3. Company websites</li> </ol>	These often pertain to marketing/prospecting activities. They can also apply to internal and other communications
<b>External organizations</b>	Organizations, except customers and suppliers, external to the company	<ol style="list-style-type: none"> <li>1. Complementors/business partners</li> <li>2. Existing competitors</li> <li>3. Potential competitors</li> </ol>	In the paradigm of "networked organizations" of today, this inclusion is important
<b>Facilities and equipments</b>	Real estate and structures and their related components, movable machinery, devices, tools and their integrated components	<ol style="list-style-type: none"> <li>1. Buildings and surroundings</li> <li>2. Heavy machinery</li> <li>3. Testing and other equipments</li> <li>4. Factories</li> </ol>	Software that is integral to equipments is included within this area; other software is included within information area. Integrated components (e.g., security alarm system within an office or plant) are often included as a part of the facility

internal network by using the firewalls to segment the Intranet. This enables segregation of departmental Intranets; for example, a company can separate departments such as finance or accounting from the rest of the Intranet and thereby prevent infections from penetrating these critical segments of the corporate network. Figure 9.9 shows the diagram of the firewall with two demilitarized zone (DMZ) networks.

If there is a need to use an existing multiple network segments then you can deploy multiple DMZ with differing security policies (levels). For example, you may need to deploy the applications for Extranets, Intranets, web server hosting and remote access gateways (see Fig. 9.9).



e 9.9 | Firewall with DMZ networks.



Even if one of these criteria is not met, automatically, access should be denied to the device or access may be provided only on a limited basis. On the basis of necessity warranted by a situation, mobile devices can be forwarded directly to a website containing the required updates.

With the use of centralized management, administrators can manage, monitor and configure the entire network and all devices using a single management console. They can also monitor user activities on the network by viewing reports. For example, system administrators will be able to know who has accessed which data at what time. This allows preventing attacks more effectively and provides more efficient protection for corporate applications at risk. A central management console also makes it possible to roll out and maintain standard security guidelines for the entire corporate network. Given these issues, risks and challenges involved with the use of social media marketing tools, indeed the involvement of the senior employees of the organization is critical to the success of the social media marketing initiative. Although organizations scurry to social media marketing techniques remain competitive and look "modern," they should take due care to avoid loss of reputation. Organizations also ensure corporate compliance. To conclude this section, the organizational best practices are listed below:

1. Organization-wide information systems security policy;
2. configuration/change control and management;
3. risk assessment and management;
4. standardized software configurations that satisfy the information systems security policy;
5. security awareness and training;
6. contingency planning, continuity of operations and disaster recovery planning;
7. certification and accreditation (refer to Chapter 12 in CD).

## **Social Computing and the Associated Challenges for Organizations**

Social computing is also known as “Web 2.0” – it empowers people to use Web-based public products and services. Social computing is much more than just individual networking and entertainment. It helps thousands of people across the globe to support their work, health, learning, getting entertained and citizenship tasks in a number of innovative ways. In the modern era, we are “constantly connected,” business is “24 × 7” – the business where world never sleeps. People carry anxieties in a competitive business world. In such a milieu, people and organizations are appreciating the “power of social media.” Business is taken forward based on how connections are made through social networks. In this process, a lot of information gets exchanged and some of that could be confidential, Personally Identifiable Information (PII)/SPI, etc. This would be a gold mine for the cybercriminals. “Social networking,” “social media marketing” (addressed in Section 9.5) and “social computing” are not unrelated concepts. There is a new genre of challenges, though they come with rising use of social computing and organizations need to watch for these challenges. For example, social computing poses the risk of “digital divide.” Getting too used to readily available information, people may get into the mode of not questioning the accuracy and reliability of information that they readily get on the Internet. With social computing, there are new threats emerging; those threats relate to security, safety and privacy. How to protect one’s online privacy is in fact a major preoccupation for people all over the world; particularly in European countries where there is a very high consciousness about privacy loss. Impersonation and identity theft are some of the new risks as discussed in Chapter 5. Cyberbullying (explained in Box 2.8 of Chapter 2) and “online grooming” are the new emerging threats for children in particular. Over and above this, unclear data ownership and lack of controls in users hand for guarding their data are resulting into privacy invasion risks (cloud computing risks are discussed in Section 9.4).

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.



Information Security  
Education & Awareness  
Project Phase - II

# Cyber Terrorism,

- The ethical dimension of cyber crimes & psychology

**Ch A S Murty**, Associate Director,  
*Centre for Development of Advanced Computing (C-DAC)*





# Disclaimer

[www.isea.gov.in](http://www.isea.gov.in)

- This presentation is for educational and research purpose only
- Do not attempt to violate the law with anything we discussed here
- Neither the author of this material / references nor anyone else affiliated anyway, is liable for your actions



[www.cdac.in](http://www.cdac.in)

[www.  
InfoSec  
awareness.in](http://www.InfoSecawareness.in)

Toll Free No. 1800 425 6235



# Cyberspace



“A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”

-- A Definition of Cyberspace





# Defining Cyber

[www.isea.gov.in](http://www.isea.gov.in)



[www.cdac.in](http://www.cdac.in)

## Cyberspace is the connected Internet Ecosystem

- ❑ Trends Exposing critical infrastructure to increased risk:
    - Interconnectedness of Sectors
    - Proliferation of exposure points
    - Concentration of Assets
  - ❑ Cyber Intrusions and Attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy
  - ❑ Cyber Security is protecting our cyber space (critical infrastructure) from attack, damage, misuse and economic espionage
- Food & Technology
  - Commercial Facilities
  - Dams
  - Energy
  - Postal and Shipping
  - Banking and Finance
  - IT & Communication
  - Defense Industrial Base
  - National Monuments
  - Transportation
  - Chemical
  - Critical Manufacturing
  - Healthcare & Public Health
  - Nuclear Reactors
  - Water etc.,

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235



# Critical Information Infrastructures



- Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy.
- Most commonly associated with the term are facilities for:
  - Amateurs hack systems, professionals hack people. — Bruce Schneier
  - Don't assume that you're not a target. Draw up battle plans.
  - Learn from the mistakes of others





# Cyber Challenges

[www.isea.gov.in](http://www.isea.gov.in)



[www.cdac.in](http://www.cdac.in)

- ❑ Cyberspace has **inherent vulnerabilities** that cannot be removed
- ❑ **Innumerable entry points** to Internet.
- ❑ **Assigning attribution:** Internet technology makes it relatively easy to misdirect attribution to other parties
- ❑ Computer Network Defense **techniques, tactics and practices** largely protect individual systems and networks rather than critical operations (missions)
- ❑ Attack technology **outpacing** defense technology
- ❑ **Nation states, non-state actors, and individuals** are at a peer level, all capable of waging attacks



[www.  
InfoSec  
awareness.in](http://www.InfoSecawareness.in)

Toll Free No. 1800 425 6235





www.isea.gov.in

# Cyber Crime: Goal, Profile, Targets



www.cdac.in

Goals	Profile	Target and Motive
Money	State-Sponsored	Corporate
Power	Non-State	Defacement, Takeover / control
Control	Insiders	Financial , Extortion, Revenge
Publicity	Hactivists	Information / Data Theft
Revenge	Organized Gangs	Reputation Damage
Crackers	Criminals	Individual/Personal -
Learning	Hobbyists,	Yours and Family – entire life
Strategic	Learners and	Stalking, Blackmail, Scams
Espionage	Enthusiasts	Governmental / Military Secrets, Weapon Control
		Political, Religious, National unrest

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235



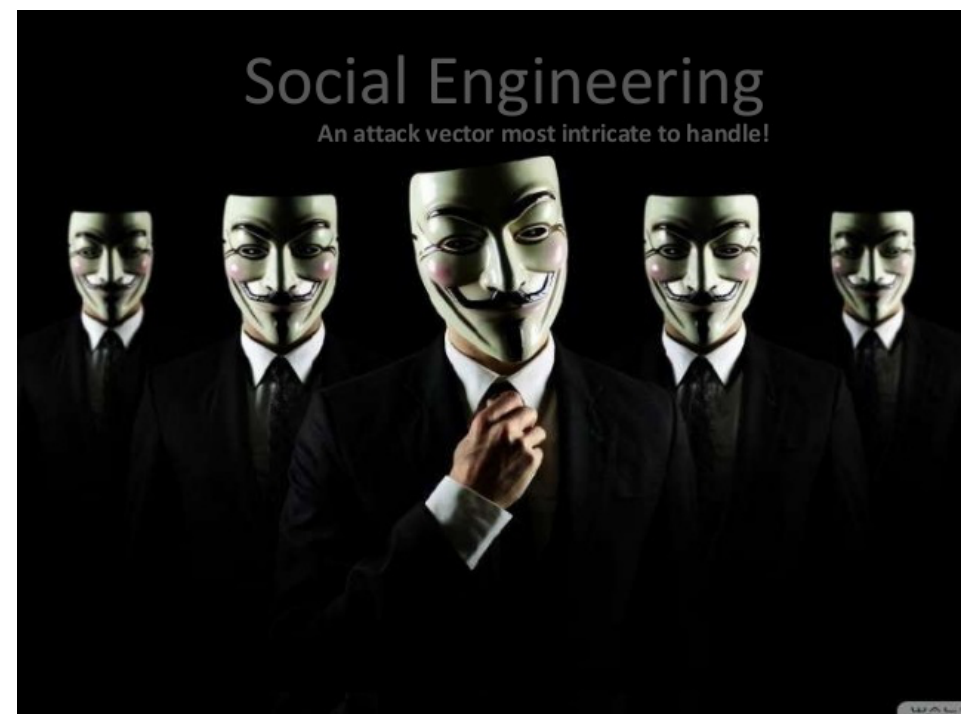
# CYBER ESPIONAGE -METHODS OF SPREADING

[www.isea.gov.in](http://www.isea.gov.in)



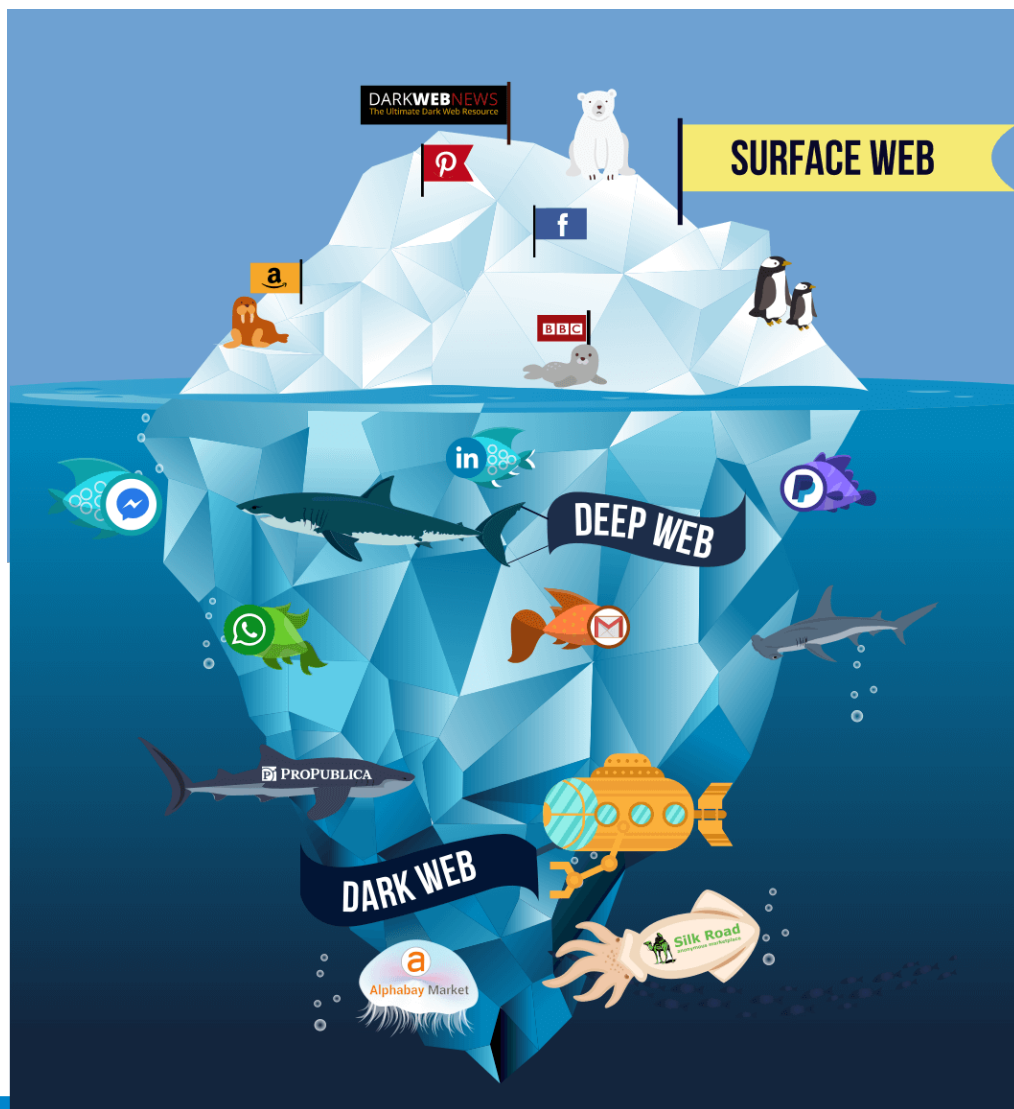
[www.cdac.in](http://www.cdac.in)

- Exploitation of vulnerabilities commonly software products, such as: Java ,Adobe Reader, Microsoft Office, Internet Explorer, Adobe Flash and more
- Social engineering techniques – including spear-phishing campaigns
- Drive-by downloads , Droppers
- The act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers
- You don't control all of your critical business systems. Understand your vulnerabilities in the distributed, outsourced world



[www.  
InfoSec  
awareness.in](http://www.InfoSecawareness.in)

Toll Free No. 1800 425 6235





www.isea.gov.in



www.cdac.in

**NIGHTMARE**

We highly recommend that you disable Javascript while on the marketplace for better security.

**Featured Listings**  
Just the best in our market...

- Dr Relax 145  
5.00★ Trust Level 6  
USD 370.55  
PURE MDMA CHAMPAGNE - 84% 50 gram
- HeinkenXpress 103  
4.98★ Trust Level 1  
USD 0.29  
3-0.25 PENCE 3...1x MY BRAND 220mg netto DREAM REFUGEE SPECIAL
- theiceman33 116  
5.00★ Trust Level 4  
USD 81.22  
THEICEMAN'S FIRE BITCH KILLER METH !!!Gram
- RAISED BY DIABLOW 560  
5.00★ Trust Level 7  
USD 141.11  
1.75g AFGHAN HEROIN & 7 SUPER LAB CRYSTAL "PARTY PACK"

- Alphen #3 Heroin - UK vendor  
\$1.82 USD - FE  
Ship to GB WW
- 1g of PELLET Cocaine  
40.10 USD - FE  
Ship to GB
- 10 x Alex Gray's Rohmann LSD Acid (10 x...)  
64.32 USD - FE  
Ship to WW
- 1g - Super Lemon Hash - AAAA+  
18.55 USD - FE  
Ship to GB
- 50 Multiple Strains A+ UK Vendor  
79.83 USD - FE  
Ship to GB
- 1.5g 2C-FE HD  
30 USD - FE  
Ship to WW
- Rohdan 20mg Rohdanil x 10 (UK...)  
20 USD - FE  
Ship to GB
- 14 High Quality Meth  
200 USD  
Ship to GB
- 40.88g - FINEST UNCUT AFGAN #3 HEROIN...  
73.42 USD - FE  
Ship to GB
- Actavis Escapem 10mg X 20 Tabs...  
43.25 USD  
Ship to GB WW

**ARMOY**

Shopping Cart: 0 item(s) - \$0.00

Categories:

- Package Deals (4)
- Pistols (87)
- Rifles (66)
- Shotguns (4)
- NFA Weapons (84)
- Accessories (68)
- Armor (28)
- Ammunition (33)
- Military (44)

**Bestsellers**

- Walther P22: \$752.65
- Glock 17 & GenTech Type F: \$2,223.48
- Beretta PX4 Storm Type F: \$1,223.90
- 9x19mm Parabellum: \$0.30
- Glock 26 Gen4: \$1,027.34
- Glock 17 Gen4: \$1,027.34
- CIA Model PAP: \$1,466.44
- Glock 32 Gen4: \$1,027.34

**BlackMarket Reloaded**

Categories: Drugs (2664), Services (971), Data (549), Weapons (301), Collectables (148), Metals/Stones (131), Other (116), Software (113), Movies (14), Tobacco (178), Counterfeits (124), Alcohol (47)

**Weapons & Firearms**

Ak-47, decent condition

Price: 103.89610 BTC  
€ 1,478.09 | £ 2,000.00 | \$ 2,269.60

Ship from: USA, Philadelphia  
Ship to: Worldwide  
Stock: 1

Created in: 2012-06-30 03:12 UTC  
Last update: 2012-12-11 01:47 UTC

Your balance isn't enough to buy this item! Please deposit the needed funds before.

**3MIG**

Weapons & Firearms

AK-47, decent condition

Price: 103.89610 BTC

Ship from: USA, Philadelphia  
Ship to: Worldwide  
Stock: 1

Created in: 2012-06-30 03:12 UTC  
Last update: 2012-12-11 01:47 UTC

Toll Free No. 1800 425 6235





# Underground Cyber Market

[www.isea.gov.in](http://www.isea.gov.in)



[www.cdac.in](http://www.cdac.in)

- The Internet is where everyone has access to and where it's easy to find things because they're indexed by search engines.
- The Deep Web is the part of the Internet that isn't necessarily malicious, but is just too obscure to be indexed due to the sheer size of the web. Approx. 96 % of the internet is beyond search engines such as Google and Bing
- The Dark Web is the part of the non-indexed part of the Internet (the Deep Web) that is used by those who don't want to be found for whatever reason. This could be for seedy, illegal purposes or it could be a matter of privacy. C3 : Cyber-crime , Cyber-war , Cyber-terrorism
- Silk Road provided a platform for drug dealers around the world to sell narcotics through the Internet
  - 950,000+ registered user • Taken down Sep 2013
  - Dark market facilitated the buying & selling of stolen financial information
  - Had 2500+ members
  - Taken down in 2010 Sites like Silk Road and DarkMarket operate in the Deep Web / Dark Web offering illegal services

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235



# Cyber War

[www.isea.gov.in](http://www.isea.gov.in)



[www.cdac.in](http://www.cdac.in)

A Lot of Folks Have Substantial Misconceptions About This "Cyber War" Thing

- Cyber war is NOT about only “inadvertent” nuclear war
- Cyber war is NOT about only cyber intrusions –
- Cyber war is NOT about only defacing web sites –
- Cyber war is NOT about only DDoS attacks –
- Cyber war is NOT about only malware –
- Cyber war is NOT about only cyber-enabling regular terrorism –
- Cyber war is NOT about “high tech” war that isn't computer or network focused, nor is it about “non-technical” military information operations
- That’s all “bad stuff,” and it might be “cyber espionage,” or “cyber terrorism,” or “high tech war” or "nuclear war" or "regular war" but it’s not cyber war.

However since a lot of the impressions we have about cyber war are formed around those misconceptions, we need to start by looking at those areas



[www.  
InfoSec  
awareness.in](http://www.InfoSecawareness.in)

Toll Free No. 1800 425 6235



www.isea.gov.in

# Data Breaches



www.cdac.in

**Adobe (2013)** -  
150 million records

**My Fitness Pal**  
**Date:** February 2018  
**Impact:** 150 million user accounts

**Adult Friend Finder (2016)** –  
412.2 million accounts

**Equifax**  
**Date:** July 29, 2017  
**Impact:** 147.9 million consumers

**Yahoo**  
**Date:** 2013-14  
**Impact:** 3 billion user accounts

**CANVA**  
May 2019  
**Impact:** 137 million user accounts

**Dubsmash**  
**Date:** December 2018  
**Impact:** 162 million user accounts

**Marriott International**  
**Date:** 2014-18  
**Impact:** 500 million customers

**eBay**  
**Date:** May 2014  
**Impact:** 145 million users

**Heartland Payment Systems**  
**Date:** March 2008  
**Impact:** 134 million credit cards exposed

**Zynga**  
**Date:** September 2019  
**Impact:** 218 million user accounts

**LinkedIn**  
**Date:** 2012 (and 2016)  
**Impact:** 165 million user accounts

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235



www.isea.gov.in



www.cdac.in

**Hackers steal healthcare records of 6.8 million Indian citizens**

**Date:** August 2019

**Impact:** 68 lakh patient and doctor records

**Local search provider JustDial exposes data of 10 crore users**

**Date:** April 2019

**Impact:** personal data of 10 crore users released

**SBI data breach leaks account details of millions of customers**

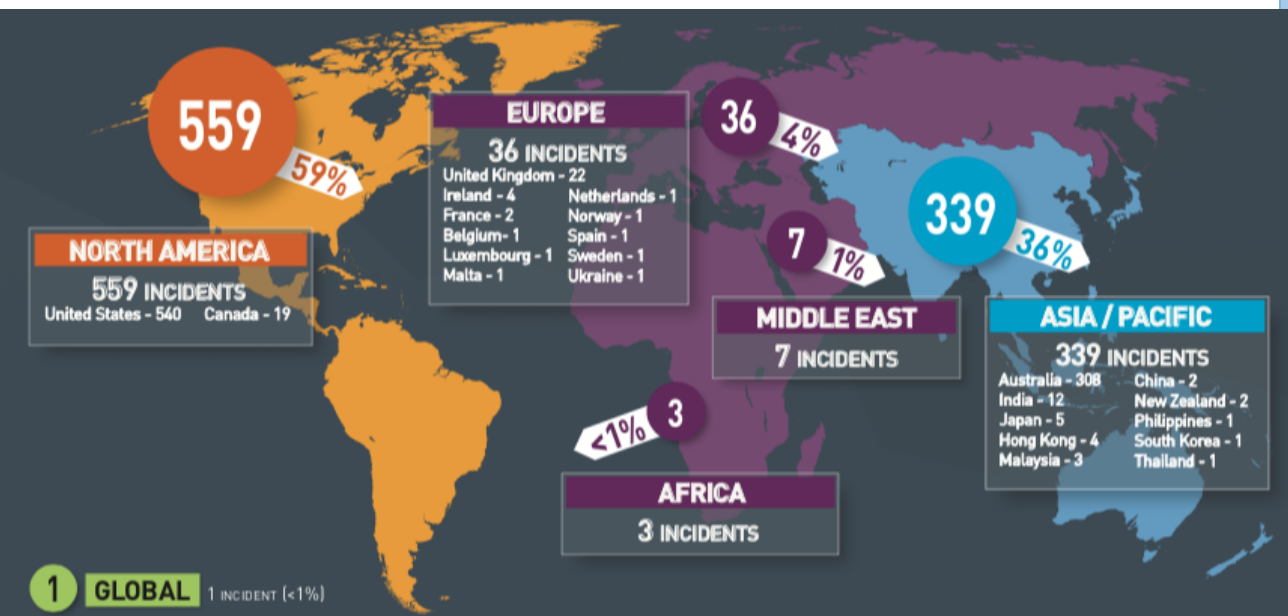
**Date:** January 2019

**Impact:** three million text messages sent to customers divulged

**Unacademy learns lesson about security**

**Date:** May 2020

**Impact:** 22 million user accounts



www.**InfoSec**awareness.in

Toll Free No. 1800 425 6235





# Organized Cyber Crime

www.isea.gov.in



www.cdac.in

- Cyber organized criminals have engaged in a variety of cybercrimes including
  - fraud,
  - hacking,
  - malware creation and distribution,
  - DDoS attacks,
  - blackmail, and
  - intellectual property crime
    - the sale of counterfeit or
    - falsified trademarked products

- These types of cybercrimes cause
  - financial,
  - psychological,
  - economic, and even physical harm (especially counterfeit electronics and automobile parts, as well as falsified medical products, defined by the World Health Organization as "deliberately/ fraudulently misrepresent their identity, composition or source," see WHO, 2017), and
  - have been used to fund other forms of serious crime, such as terrorism

- Albanese, 2018; Europol, 2018; Broadhurst et al., 2018; Maras, 2016
- Organized criminal groups have also profited and/or otherwise benefited from illicit products and services offered online. For example, the creator of the Butterfly Bot advertised this malware online as capable of taking control of Windows and Linux computers

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235



# Five Types of Terrorism



You will need to be familiar with the five types of terrorism.

- **State-Sponsored terrorism**, which consists of terrorist acts on a state or government by a state or government.
- **Dissent terrorism**, which are terrorist groups which have rebelled against their government.
- **Terrorists and the Left and Right**, which are groups rooted in political ideology.
- **Religious terrorism**, which are terrorist groups which are extremely religiously motivated and
- **Criminal Terrorism**, which are terrorists acts used to aid in crime and criminal profit.



# Cyber Terrorism: An Introduction



Cyber-crime, Info war, Net war, cyber terrorism, Cyber harassment, Virtual warfare, digital terrorism, cyber tactics, Computer Warfare, cyber attack, and cyber-break-ins is used to describe what some military and political strategists describe as the “**new terrorism**” of our times.

“The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner.”

Ban Ki-moon,  
The eighth Secretary-General of the United Nations



# Cyber Terrorism: An Introduction

[www.isea.gov.in](http://www.isea.gov.in)



[www.cdac.in](http://www.cdac.in)

- Cyber terrorism is the convergence of cyberspace and terrorism.
- It refers to **unlawful attacks** and threats of attacks against computers, networks and the information stored therein when done **to intimidate** or **coerce a government** or **its people in furtherance** of political or social objectives.
- Further, to qualify as cyber terrorism, an **attack should result in violence** against persons or property, or **at least cause enough harm to generate fear**.
  - Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact.
  - Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235



# Cyber terrorism Vs. Hacktivism



It is important to distinguish between cyberterrorism and “hacktivism,” a term coined by scholars to describe the marriage of hacking with political activism.

“Hacking” is here understood to mean activities conducted online and covertly that seek to reveal, manipulate, or otherwise exploit vulnerabilities in computer operating systems and other software.

Unlike hacktivists, hackers tend not to have political agendas.

Hactivists have four main weapons at their disposal:

- Virtual blockades;
- e-mail attacks;
- Hacking and computer break-ins; and
- Computer Viruses and Worms.



[www.isea.gov.in](http://www.isea.gov.in)

# Is Cyberterrorism is an attractive option?



[www.cdac.in](http://www.cdac.in)

it is cheaper than traditional terrorist methods

Cyber terrorism is more anonymous than traditional terrorist methods

The variety and number of targets are enormous. The cyber terrorist could target the computers and computer networks of governments, individuals, public utilities, private airlines, and so forth

Cyber terrorism can be conducted remotely, a feature that is especially appealing to terrorists

Cyber terrorism has the potential to affect directly a larger number of people than traditional terrorist methods



[www.InfoSecawareness.in](http://www.InfoSecawareness.in)



Toll Free No. 1800 425 6235





www.isea.gov.in

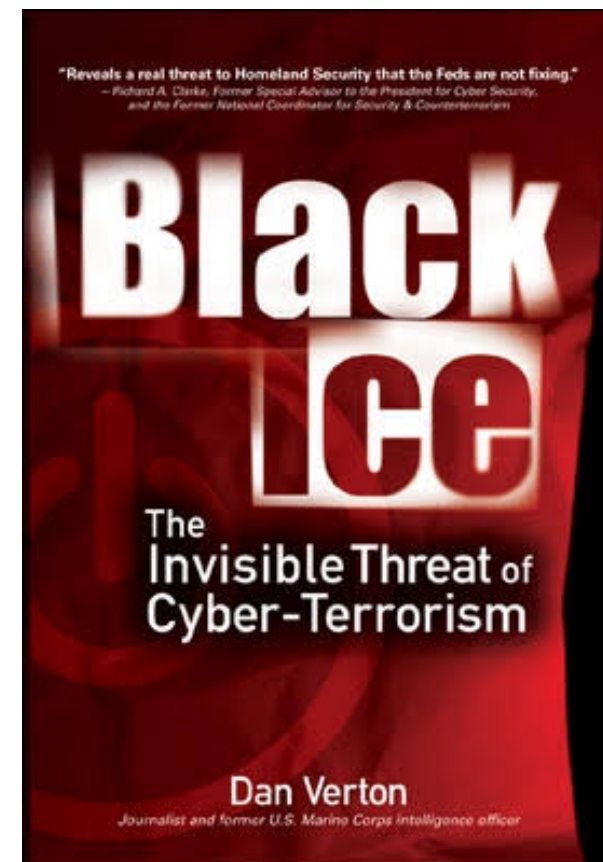
# The hackers managed to gain access to dozens of critical Pentagon computer systems



www.cdac.in

Black Ice: The Invisible Threat of Cyber-Terror, a book published in 2003  
**The 1997 exercise code-named “Eligible Receiver,” conducted by the National Security Agency (NSA).**

- The exercise began when NSA officials instructed a “Red Team” of thirty-five hackers to attempt to hack into and disrupt U.S. national security systems
- They were told to **play the part of hackers** hired by the **North Korean intelligence service**, and their primary target was to be the U.S. Pacific Command in Hawaii.
- They were allowed to penetrate any Pentagon network but were prohibited from breaking any U.S. laws
- They could only use hacking software that could be downloaded freely from the Internet



Once they entered the systems, they could easily create user accounts, delete existing accounts, reformat hard drives, scramble stored data, or shut systems down. They broke the network defenses with relative ease and did so without being traced or identified by the authorities.

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235



In March 2000, Japan’s Metropolitan Police Department reported that a software system they had procured to track 150 police vehicles, including unmarked cars, had been developed by the Aum Shinryko cult,

the same group that gassed the Tokyo subway in 1995, killing 12 people and injuring 6,000 more.

- At the time of the discovery, the cult had received classified tracking data on 115 vehicles.
- Further, the cult had developed software for at least 80 Japanese firms and 10 government agencies. They had worked as subcontractors to other firms, making it almost impossible for the organizations to know who was developing the software.
- As subcontractors, the cult could have installed Trojan horses to launch or facilitate cyber terrorist attacks at a later date.

32°C M/SUNNY  
 TOKYO (5 p.m.)  
 MARKETS 106.14 ¥/\$ (4 p.m.)

# thejapan times

NEWS	OPINION	LIFE	COMMUNITY
	NATIONAL	ASIA PACIFIC	BUSINESS
		WORLD	REFERENCE
			COLUMNS

**NATIONAL**

## Agencies examine software supplied by Aum-linked firms

SHARE Mar 2, 2000

Government agencies and major companies opted to double check various computer systems Wednesday after it was discovered that some of the the software may have been developed by a firm controlled by Aum Shinrikyo.

A Ground Self-Defense Force communications system was not put into scheduled operation Wednesday after it was revealed that the firewall of the software in question was made penetrable in its development stage.

Member firms of the Nippon Telegraph and Telephone Corp. group have announced that they will stop using computer-system software allegedly developed by firms linked to the Aum Shinrikyo cult if the reports are confirmed, NTT said Wednesday.

“Should we find such software . . . as a result of checks, we will replace it,” NTT President Junichiro Miyazu told a news conference.

Four NTT group companies reportedly placed a total of 10 orders for computer systems with software development companies linked to the cult.

As a general rule, NTT “follows a policy of allowing developers to supply, as long as we find they conform to our technological specifications and are cheap,” Miyazu said.





# Black Out Day

[www.isea.gov.in](http://www.isea.gov.in)



[www.cdac.in](http://www.cdac.in)

- ❑ It was first cyber war at “New York” city on 14th, August, 2003
  - ❑ Real incidents that horribly suffered New York for 3 days
  - ❑ The hacker attacks on power lines
  - ❑ Before 3 days some one some where realize the virus named as “BLASTER” and it a self active
  - ❑ 100 power plants are shut down × By the incident effects on whole traffic ,air line power ,water system & nuclear reactor too
  - ❑ New York government struggled 3 months to find the accused



That was Russian government is totally responsibility to this act

[www.  
InfoSec  
awareness.in](http://www.InfoSecawareness.in)

Toll Free No. 1800 425 6235



# Cyber Terrorism

[www.isea.gov.in](http://www.isea.gov.in)



[www.cdac.in](http://www.cdac.in)

- 9/11 Twin Towers Attack
- Al-Qaeda laptop was found in Afghanistan.
- Hits on web sites that contained “Sabotage Handbook”.
  - Al-Qaeda actively researched publicly available information concerning critical infrastructures posted on web sites.

## Ahmedabad Bomb Blast(26-07-2008)

- A mail with id alarbi\_gujrat@ yahoo.com was being sent by a group of Terrorists.
- Person named Kenneth Haywood’s unsecured WIFI router in his house was being misused by terrorists.
- 3 more mails were sent after the blast with the same misuse of unsecured WIFI routers.

- 26/11 Mumbai Attack
- Terrorists communicated with handlers in Pakistan through Callphone using VoIP (Voice over Internet Protocol).
- The accused communicated to terrorists with an email id Kharak\_telco@yahoo.com which was accessed from 10 different IP addresses

[www.  
InfoSec  
awareness.in](http://www.InfoSecawareness.in)

Toll Free No. 1800 425 6235



# Cyber Space Role

[www.isea.gov.in](http://www.isea.gov.in)



[www.cdac.in](http://www.cdac.in)

Since the late 1980s, the Internet has proven to be a highly dynamic means of communication, reaching an ever-growing audience worldwide

Internet technology makes it easy for an individual to communicate with relative anonymity, quickly and effectively across borders, to an almost limitless audience

The development of increasingly sophisticated technologies has created a network with a truly global reach, and relatively low barriers to entry.

The benefits of Internet technology are numerous, starting with its unique suitability for sharing information and ideas, which is recognized as a fundamental

It must also be recognized,

However, that the same technology that facilitates such communication can also be exploited for the purposes of terrorism.

The use of the Internet for terrorist purposes creates both challenges and opportunities in the fight against terrorism.

[www.  
InfoSec  
awareness.in](http://www.InfoSecawareness.in)

Toll Free No. 1800 425 6235



# Cyber Terrorism in India ???



ECIL(Electronic Corporation of India Limited) which was invented electro voting system in India , controlling parliament security system , Nuclear plants ,Defense etc.

- ECIL CYBER website was hacked by Phrozenmyst
- Not only ECIL and also ISRO ,BARC
- The hacker Phrozenmyst was stolen sensitive data from ECIL and pasted on PAGEBIN website
- Due to they are making some illegal tenders and he tweet on his tweeter account
- From 2010 to Pakistan and china attacking the India by cyber
- Recently Pakistan is made a successfully attack on India by an fake currency at elections time

Cyber Attacks on India are Increasing with Rapid Growth of 200%+ /Year.

- Hack Your Life ultimately ~ Hack your nation
- CYBERCRIME - When a Cyber-attack is use to Steal Money HACTIVISM When one uses Cyber-attack to promote Political Agendas
- CYBER ESPIONAGE - When Cyber-attack is used to steal Specific Information
- CYBER WARFARE When Cyber-attack is used to form terrorism against Govt. ,Nation



# Means by which Cyber Space is utilized for terrorist purposes



the Internet is often utilized to promote and support acts of terrorism in following six sometimes overlapping categories:

- **Propaganda** (including recruitment, radicalization and incitement to terrorism);
- **Financing;**
- **Training;**
- **Planning** (including through secret communication and open-source information);
- **Execution;** and
- **Cyberattacks.**

- Propaganda generally takes the form of multimedia communications providing
  - ideological or Practical instruction,
  - Explanations,
  - justifications or
  - Promotion of Terrorist Activities.
- These may include virtual messages, presentations, magazines, treatises, audio and video files and video games developed by terrorist organizations or sympathizers.
- intended and likely to incite acts of violence against individuals or specific groups of individuals
- **The promotion of violence is a common theme in terrorism-related propaganda.**



www.isea.gov.in

# Means by which Cyber Space is utilized for terrorist purposes



www.cdac.in

The Internet is often utilized to promote and support acts of terrorism in following six sometimes overlapping categories:

- **Propaganda** (including recruitment, radicalization and incitement to terrorism);
- **Financing;**
- **Training;**
- **Planning** (including through secret communication and open-source information);
- **Execution;** and
- **Cyberattacks.**

Terrorist organizations and supporters may also use the Internet to finance acts of terrorism.

Direct Solicitation, e-commerce, the exploitation of online payment tools and through charitable organizations.

Online payment facilities may also be exploited through fraudulent means such as identity theft, credit card theft, wire fraud, stock fraud, intellectual property crimes and auction fraud.

the registration by Tsouli of 180 websites hosting Al-Qaida propaganda videos and to provide equipment for terrorist activities in several countries. 1400 credit cards – 1.6 million pounds of illicit funds

Financial support provided to seemingly legitimate organizations, such as charities, may also be diverted for illicit purpose

Established shell corporations, disguised as philanthropic undertakings, to solicit online donations

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235





# Means by which Cyber Space is utilized for terrorist purposes

www.isea.gov.in



www.cdac.in

the Internet is often utilized to promote and support acts of terrorism in following six sometimes overlapping categories:

- **Propaganda** (including recruitment, radicalization and incitement to terrorism);
- **Financing;**
- **Training;**
- **Planning** (including through secret communication and open-source information);
- **Execution;** and
- **Cyberattacks.**

In recent years, terrorist organizations have increasingly turned to the Internet as an alternative training ground for terrorists.

Growing range of media that provide platforms for the dissemination of practical guides in the form of online manuals, audio and video clips, information and advice

Inspire is an online magazine allegedly published by Al-Qaida in the Arabian Peninsula with the stated objective of enabling Muslims to train for jihad at home

The fall 2010 edition included practical instructional material on how to adapt a four-wheel-drive vehicle to carry out an attack on members of the public

Instructional material available online includes tools to facilitate counter-intelligence and hacking activities and to improve the security of illicit communications

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235



# Means by which Cyber Space is utilized for terrorist purposes

www.isea.gov.in



www.cdac.in

the Internet is often utilized to promote and support acts of terrorism in following six sometimes overlapping categories:

- **Propaganda** (including recruitment, radicalization and incitement to terrorism);
- **Financing;**
- **Training;**
- **Planning** (including through secret communication and open-source information);
- **Execution;** and
- **Cyberattacks.**

criminal justice practitioners have indicated that almost every case of terrorism prosecuted involved the use of Internet technology

from France, Public Prosecutor v. Hicheur,<sup>15</sup> illustrates how different forms of Internet technology may be used to facilitate the preparation of acts of terrorism, including via thorough communications

Steps may also be taken via the Internet to identify a potential target of an attack and the most effective means of achieving the terrorist purpose

Preparatory secret communication

**A simple online e-mail account may be used by terrorists for electronic, or virtual, “dead dropping” of communications**

**Encryption tools and anonymizing software are readily available**

Organizations and individuals often publish extensive amounts of information on the Internet.

individuals also publish, voluntarily or inadvertently, an unprecedented amount of sensitive information on the Internet www.

**InfoSec**  
awareness.in





# Means by which Cyber Space is utilized for terrorist purposes

www.isea.gov.in



www.cdac.in

the Internet is often utilized to promote and support acts of terrorism in following six sometimes overlapping categories:

- **Propaganda** (including recruitment, radicalization and incitement to terrorism);
- **Financing;**
- **Training;**
- **Planning** (including through secret communication and open-source information);
- **Execution;** and
- **Cyberattacks.**

explicit threats of violence, including in relation to the use of weapons, may be disseminated via the Internet to induce anxiety, fear or panic in a population or subset of the population

Internet communications may also be used as a means to communicate with potential victims or to coordinate the execution of physical acts of terrorism. For example, the Internet was used extensively in the coordination of participants in the attacks of 11 September 2001 in the United States

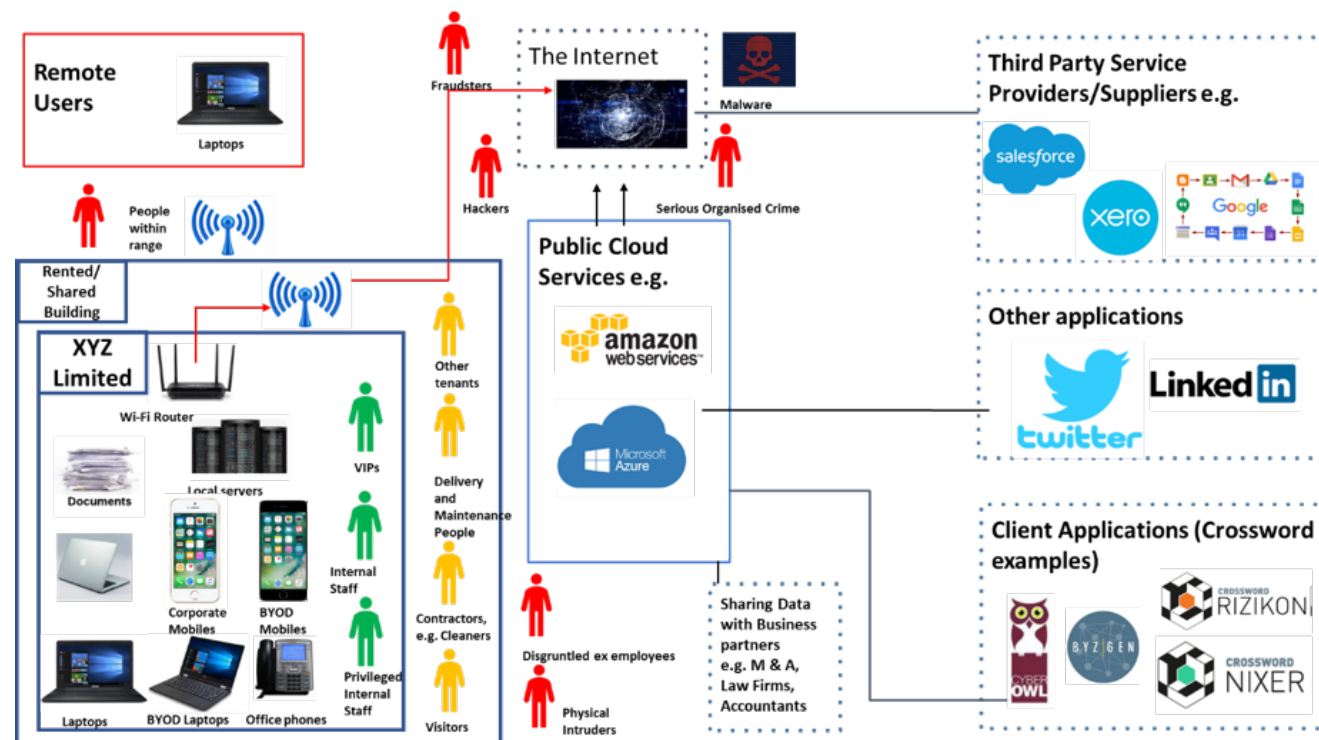
The use of the Internet in furtherance of the execution of acts of terrorism may, inter alia, offer logistical advantages, reduce the likelihood of detection or obscure the identity of responsible parties

Terrorists may purchase individual components or services required to perpetrate violent acts of terrorism by means of electronic commerce

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235

- Air traffic control towers or our airlines infrastructure could be hacked into.
- Banking systems could be violated and all of our money could be stolen.
- Bombs and other explosives could be set off by remote.
- Hospitals could lose all of their information.
- Learn Government secrets and plans
- The tampering of our water systems.





[www.isea.gov.in](http://www.isea.gov.in)



[www.cdac.in](http://www.cdac.in)

## **Cyber security countermeasures to combat cyber terrorism**

[L. Mackinnon, L. Bacon, +3 authors D. Frangiskatos](#)

## **Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes**

[Michael L. Gross, Daphna Canetti, Dana R. Vashdi](#)

Cyber Terrorism: Its Effects on Psychological Well Being, Public Confidence and Political Attitudes (March 2016) -

[Michael L GrossDaphna Canetti](#)Dana Vashdi

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235



# What do we need to do??

[www.isea.gov.in](http://www.isea.gov.in)



[www.cdac.in](http://www.cdac.in)

- Maintain high alert & vigilance.
- Update OS and applications regularly.
- Enforce strong passwords.
- "Lock down" systems.
- Keep anti-virus software installed and up-to- date.
- Employ intrusion detection systems and firewalls.
- Prevention & Protection:
  - Be cautious about opening email attachments.
  - Complete Software Updates
  - Create difficult passwords
  - Download updated anti-virus software
  - Uninstall unused applications or services

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235



[www.isea.gov.in](http://www.isea.gov.in)

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235

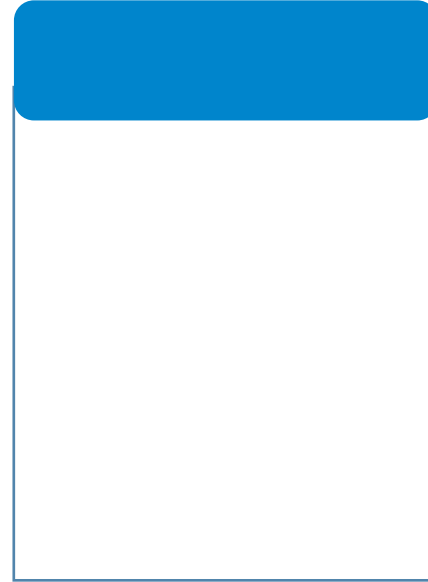
# References

- <https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html>
- <https://www.cisa.gov/cyber-storm-vi>
- <https://www.usip.org/sites/default/files/sr119.pdf>
- <https://www.slideshare.net/Deepakniit14/c3-11-sep>
- <https://www.slideshare.net/tejesh002/cyber-terrorism-36520078>



[www.isea.gov.in](http://www.isea.gov.in)

[www.  
InfoSec  
awareness.in](http://www.InfoSecawareness.in)



Toll Free No. 1800 425 6235



[www.isea.gov.in](http://www.isea.gov.in)

www.  
**InfoSec**  
awareness.in

Toll Free No. 1800 425 6235



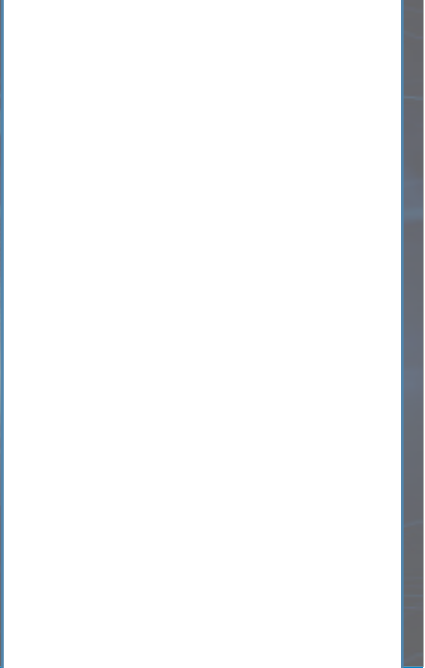
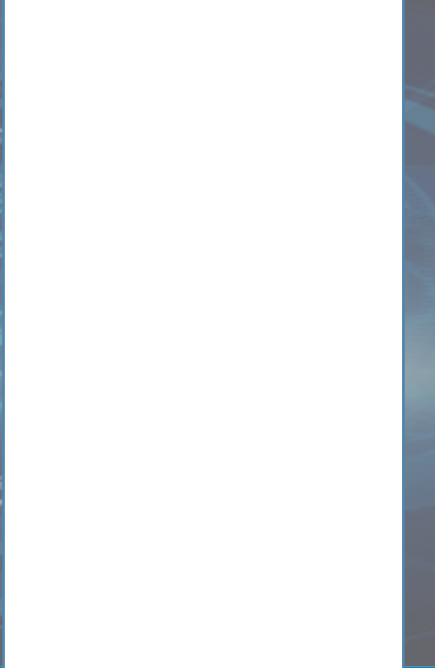
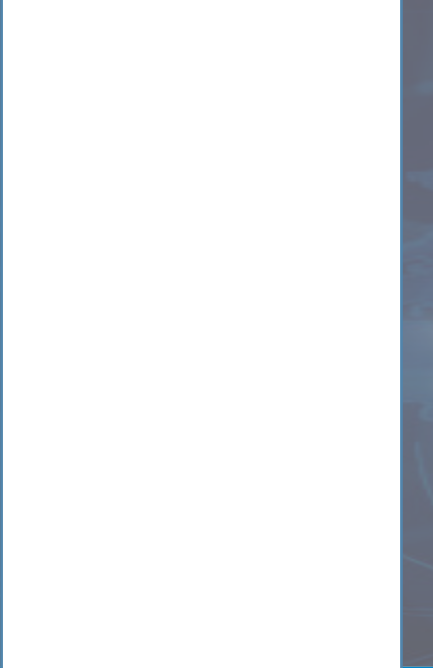


[www.isea.gov.in](http://www.isea.gov.in)

[www.  
InfoSec  
awareness.in](http://www.InfoSecawareness.in)



Toll Free No. 1800 425 6235



## UNIT - V

# Fundamental Concepts of Data Privacy

## What is Data Privacy?

**Data privacy** or Information privacy is concerned with **proper handling, processing, storage and usage of personal information**. It is all about the rights of individuals with respect to their personal information.

**The most common concerns regarding data privacy are:**

- Managing contracts or policies,
- applying governing regulation or law (like General Data Protection Regulation or GDPR),
- Third-party management.

**Privacy, in general**, is an individual's right to freedom from intrusion and prying eyes or the right of the person to be left alone.

Data Privacy describes the practices which ensure that the data shared by customers is only used for its intended purpose. In a world with ever-growing mountains of big data, privacy is an increasing topic of scrutiny.

Data privacy laws such as the United States' Health Insurance Portability and Accountability Act (HIPAA) govern specific types of data.

Other examples like the Electronic Communications Privacy Act (ECPA) extend government restrictions on wiretaps to include transmissions of electronic data.

The Children's Online Privacy Protection Act (COPPA) gives parents control over what information websites can collect from their kids.

While the EU's General Data Protection Regulation (GDPR) gives citizens new control over their data and their interactions with companies. Compliance officers within an organization are responsible for designing a data privacy policy so understanding data privacy regulations like these is a key element of the role.

## Why is Data Privacy Important?

The ability to deliver and enforce a healthy company data privacy policy is growing in importance as a measure of trust. Information privacy is becoming more complex by the minute.

The sophisticated nature of technological development means new kinds of personal data are being collected from customers and citizens.

Jurisdictions including federal, states, and international bodies like the European Union are enacting new data privacy regulations.

New regulations get enacted thanks to growing awareness among citizens and lawmakers who may not be data or technical experts.

High-profile data breaches have created heightened concern about how data may be protected and kept private.

Most regulators can exact hefty fines to enforce their data privacy requirements.

Consumer and regulator concern about protecting sensitive data means jurisdictions are passing new data privacy acts and penalties to enforce them.

## **What are the Benefits of Complying with Data Privacy Laws?**

Healthy data privacy programs which protect data and personally identifiable information have a number of benefits for organizations.

First, the fines and penalties written into data privacy regulations can be quite steep. For example, under the EU's General Data Protection Regulation (GDPR), organizations can be fined 4% of annual global revenue or 20 million euros.

Beyond the potential punitive costs, cost-savings are possible benefits of a program that addresses key data privacy issues.

Data protection regulations like GDPR require not only safeguarding user data, but also responding and sharing data upon request.

Clean, efficient processes for the organization to meet these data governance obligations can reap substantial cost-savings.

In January 2019, Cisco reported that two-thirds of companies say they are seeing sales delays due to data privacy questions from their customers. Violations of data privacy erode consumer, investor, and stakeholder trust in the organization.

When a stakeholder has doubts about the organization's ability to prevent identity theft, they may be unwilling to conduct business with that organization. Conversely, this awareness makes people more likely to do business with organizations that understand their obligations under consumer data privacy laws.

An organization that demonstrates a solid understanding of data privacy principles is often seen as a leader in their category.

Healthy data privacy programs are only possible with investment and support from the leadership team. Smart corporate board directors will grasp the value of this approach.

## **Data Privacy vs Data Security?**

Data privacy and data security are separate but related concepts. Both data security and privacy relate to control of the user's data. However they have distinct meanings. Data security is the policies and procedures that apply to protecting sensitive data stored within the company from malicious intruders. These policies help ensure data confidentiality, integrity and availability.

Data privacy principles are the policies and procedures governing who may access the data. This includes people within the organization or department that has been granted access. Therefore, it's possible to have a healthy security stance without addressing data privacy basics. However, it's not possible to ensure data privacy without a solid security stance.

## **How important is Data Privacy?**

Data privacy is arguably one of the most important considerations in a company's compliance program. Some data protection regulations have enforcement fines attached to them. Others have regulatory orders overseeing them for as many as 20 years. Guided by these laws and regulations, it behooves the organization to develop a healthy program to protect sensitive data.

Organizations that implement a healthy data privacy program reduce the number of security incidents that result in privacy breaches. Fewer breaches mean the business does not lose trust. Guarding against this erosion of trust is important to prevent losing customers or other types of business. It also saves the business from fines, multi-year penalties, or civil suits which often follow on significant breaches.

Besides an impact on the business, consider that data privacy issues can hurt the individuals affected. Loss of personally identifiable information can negatively impact individual users, customers or citizens. Cases have been reported of data subjects dealing with breach and privacy problems for decades after data loss. Beyond the punitive impacts enshrined in data protection regulations, an organization may be held liable by the individual for these issues.

Forbes reported in 2014 that 46% of organizations suffered damage to their reputation and brand value as a result of a privacy breach. The benefits of complying with data privacy laws grow in clarity every day in a world where new jurisdictions are passing their own data protection regulations.

## **Examples of Data Privacy Risks?**

In order to secure a data privacy certification from one of the trusted audit organizations, such as ISO, SOC II, or HIPAA compliance, an organization must show they prevent data privacy risks. Some key examples of cloud data privacy challenges can include:

- 1. Vulnerabilities in Web Applications**  
Any software hosted in the cloud or on the web should be fully vetted and secure before deploying within an otherwise secure organization. Have a data privacy compliance checklist to protect your program before installing something new.
- 2. Insiders and Poorly-Trained Employees**  
Every member of your team should be fully trained and aware of the data privacy basics for which they are responsible. Care given to crafting and enforcing a corporate data privacy policy can ensure this is successful.
- 3. Lacking Breach Response**  
An important part of a data privacy compliance program is an incident response plan. Make sure we have a clear plan in place, rehearsed, and that the command line is ready to deploy this plan when any issues arise.
- 4. Inadequate Personal Data Disposal**  
Personal data should be kept only as long as the relationship with the customer or employee (and related legal obligations) are in effect. Your organization can incur significant fines under the EU's General Data

Protection Regulation (GDPR) if this program does not perform this function.

5. **Lack of Transparency in Privacy Policies, Terms and Conditions**  
Ensure every customer, vendor, user or investor can understand your privacy policies, terms and conditions. Ensure they are clear on what they are agreeing to, and on the obligations to which they are subscribing.
6. **Collection of Unnecessary Data**  
collecting data should always be done with a specific purpose for which consent has been received. Most data protection laws and regulations mandate an organization may not collect more data than is required for the transaction. A data privacy consent form can help explain your company's policies and what the user is consenting to.
7. **Personal Data Sharing**  
Be sure to inform all users before any personally identifiable information leaves the database in your organization for which permission has been granted.
8. **Incorrect or Outdated Personal Data**  
Individuals have the right to rectify outdated or uncorrected personal data under most data privacy laws and regulations. This is an important update in data privacy protection. Ensure your organization has a specific policy and actionable procedures in place to allow users to exercise this right.
9. **Session Expiration Problems**  
when a data subject provides personal information to a web application, session expiration can create risk. If a data subject abandons their session and their data is exposed, the organization may be held liable for this cloud data privacy breach.
10. **Data transfer Over Insecure Channels**  
Always use secure channels and protocols (e.g. SFTP, TLS) to transmit sensitive data. When data is exposed through insecure channels (e.g. FTP, HTTP), incidents can occur.
11. **Extra Credit: Dealing With the Unknown**  
Ensure your team, procedures, and command line are prepared for unexpected contingencies. The big data privacy challenges of the modern business landscape present new threats and compliance challenges on a

regular basis. A healthy program for data governance security and privacy can adapt and adjust to keep your organization compliant and secure.

## **Data Privacy Attacks**

### **What is a Data Breach?**

A data breach is the release of confidential, private, or otherwise sensitive information into an unsecured environment. A data breach can occur accidentally, or as the result of a deliberate attack.

### **Biggest data breaches**

#### **1. Adobe**

Date: October 2013

Impact: 153 million user records

Details: As reported in early October of 2013 by security blogger Brian Krebs, Adobe originally reported that hackers had stolen nearly 3 million encrypted customer credit card records, plus login data for an undetermined number of user accounts.

Later that month, Adobe raised that estimate to include IDs and encrypted passwords for 38 million “active users.” Krebs reported that a file posted just days earlier “appears to include more than 150 million username and hashed password pairs taken from Adobe.” Weeks of research showed that the hack had also exposed customer names, IDs, passwords and debit and credit card information.

An agreement in August 2015 called for Adobe to pay a \$1.1 million in legal fees and an undisclosed amount to users to settle claims of violating the Customer Records Act and unfair business practices. In November 2016, the amount paid to customers was reported at \$1 million.

#### **2. Adult Friend Finder**

Date: October 2016

Impact: 412.2 million accounts

Details: This breach was particularly sensitive for account holders because of the services the site offered. The FriendFinder Network, which included casual hookup and adult content websites like Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com, was breached in mid-October 2016. The stolen



data spanned 20 years on six databases and included names, email addresses and passwords.

The weak SHA-1 hashing algorithm protected most of those passwords. An estimated 99% of them had been cracked by the time LeakedSource.com published its analysis of the data set on November 14, 2016.

As CSO reported at the time that, “A researcher who goes by 1x0123 on Twitter and by Revolver in other circles posted screenshots taken on Adult Friend Finder (that) show a Local File Inclusion vulnerability (LFI) being triggered.” He said the vulnerability, discovered in a module on the production servers used by Adult Friend Finder, “was being exploited.”

### **3. Canva**

Date: May 2019

Impact: 137 million user accounts

Details: In May 2019 Australian graphic design tool website Canva suffered an attack that exposed email addresses, usernames, names, cities of residence, and salted and hashed with bcrypt passwords (for users not using social logins — around 61 million) of 137 million users. Canva says the hackers managed to view, but not steal, files with partial credit card and payment data.

The suspected culprit(s) — known as Gnosticplayers — contacted ZDNet to boast about the incident, saying that Canva had detected their attack and closed their data breach server. The attacker also claimed to have gained OAuth login tokens for users who signed in via Google.

The company confirmed the incident and subsequently notified users, prompted them to change passwords, and reset OAuth tokens. However, according to a later post by Canva, a list of approximately 4 million Canva accounts containing stolen user passwords was later decrypted and shared online, leading the company to invalidate unchanged passwords and notify users with unencrypted passwords in the list.

### **4. eBay**

Date: May 2014

Impact: 145 million users

Details: eBay reported that an attack exposed its entire account list of 145 million users in May 2014, including names, addresses, dates of birth and encrypted passwords. The online auction giant said hackers used the credentials of three corporate employees to access its network and had complete access for 229 days—more than enough time to compromise the user database.

The company asked customers to change their passwords. Financial information, such as credit card numbers, was stored separately and was not compromised. The company was criticized at the time for a lack of communication with its users and poor implementation of the password-renewal process.

## **5. Equifax**

Date: July 29, 2017

Impact: 147.9 million consumers

Details: Equifax, one of the largest credit bureaus in the US, said on Sept. 7, 2017 that an application vulnerability in one of their websites led to a data breach that exposed about 147.9 million consumers. The breach was discovered on July 29, but the company says that it likely started in mid-May. The breach compromised the personal information (including Social Security numbers, birth dates, addresses, and in some cases drivers' license numbers) of 143 million consumers; 209,000 consumers also had their credit card data exposed. That number was raised to 147.9 million in October 2017.

Equifax was faulted for a number of security and response lapses. Chief among them was that the application vulnerability that allowed the attackers access was unpatched. Inadequate system segmentation made lateral movement easy for the attackers. Equifax was also slow to report the breach.

## **6. Dubsmash**

Date: December 2018

Impact: 162 million user accounts

Details: In December 2018, New York-based video messaging service Dubsmash had 162 million email addresses, usernames, PBKDF2 password hashes, and other personal data such as dates of birth stolen, all of which was then put up for sale on the Dream Market dark web market the following December. The information was being sold as part of a collected dump also including the likes of MyFitnessPal

(more on that below), MyHeritage (92 million), ShareThis, Armor Games, and dating app CoffeeMeetsBagel.

Dubsmash acknowledged the breach and sale of information had occurred — and provided advice around password changing — but failed to say how the attackers got in or confirm how many users were affected.

## **7. Heartland Payment Systems**

Date: March 2008

Impact: 134 million credit cards exposed

Details: At the time of the breach, Heartland was processing 100 million payment card transactions per month for 175,000 merchants — mostly small- to mid-sized retailers. The breach was discovered in January 2009 when Visa and MasterCard notified Heartland of suspicious transactions from accounts it had processed. The attackers exploited a known vulnerability to perform a SQL injection attack. Security analysts had warned retailers about the vulnerability for several years, and it made SQL injection the most common form of attack against websites at the time.

Because of the breach, the Payment Card Industry (PCI) deemed Heartland out of compliance with its Data Security Standard (DSS) and did not allow it to process payments of major credit card providers until May 2009. The company also paid an estimated \$145 million in compensation for fraudulent payments.

The Heartland breach was a rare example where authorities caught the attacker. A federal grand jury indicted Albert Gonzalez and two unnamed Russian accomplices in 2009. Gonzalez, a Cuban American, was alleged to have masterminded the international operation that stole the credit and debit cards. He was sentenced in March 2010 to 20 years in federal prison.

## **8. LinkedIn**

Date: 2012 (and 2016)

Impact: 165 million user accounts

Details: As the major social network for business professionals, LinkedIn has become an attractive proposition for attackers looking to conduct social engineering attacks. However, it has also fallen victim to leaking user data in the past.

In 2012 the company announced that 6.5 million unassociated passwords (unsalted SHA-1 hashes) were stolen by attackers and posted onto a Russian hacker forum. However, it wasn't until 2016 that the full extent of the incident was revealed. The same hacker selling MySpace's data was found to be offering the email addresses and passwords of around 165 million LinkedIn users for just 5 bitcoins (around \$2,000 at the time). LinkedIn acknowledged that it had been made aware of the breach, and said it had reset the passwords of affected accounts.

## **9. Marriott International**

Date: 2014-18

Impact: 500 million customers

Details: Marriott International announced in November 2018 that attackers had stolen data on approximately 500 million customers. The breach initially occurred on systems supporting Starwood hotel brands starting in 2014. The attackers remained in the system after Marriott acquired Starwood in 2016 and were not discovered until September 2018.

The attackers were able to take some combination of contact information, passport number, Starwood Preferred Guest numbers, travel information, and other personal information. The credit card numbers and expiration dates of more than 100 million customers were believed to be stolen, but Marriott is uncertain whether the attackers were able to decrypt the credit card numbers. The breach was eventually attributed to a Chinese intelligence group seeking to gather data on US citizens, according to a New York Times article.

## **10. My Fitness Pal**

Date: February 2018

Impact: 150 million user accounts

Details: As well as Dubsmash, UnderArmor-owned fitness app MyFitnessPal was among the massive information dump of 16 compromised sites that saw some 617 million customers accounts leaked and offered for sale on Dream Market.

In February 2018 the usernames, email addresses, IP addresses, SHA-1 and bcrypt-hashed passwords of around 150 million customers were stolen and then put up for sale a year later at the same time as Dubsmash et al. MyFitnessPal acknowledged the breach and required customers to change their passwords, but didn't share how many accounts were affected or how the attackers gained access to the data.

## **11. MySpace**

Date: 2013

Impact: 360 million user accounts

Details: Though it had long stopped being the powerhouse that it once was, social media site MySpace hit the headlines in 2016 after 360 million user accounts were leaked onto both LeakedSource (a searchable databased of stolen accounts) and put up for sale on dark web market The Real Deal with an asking price of 6 bitcoin (around \$3,000 at the time).

According to the company, lost data included email addresses, passwords and usernames for “a portion of accounts that were created prior to June 11, 2013, on the old Myspace platform.” According to Troy Hunt of HaveIBeenPwned, the passwords were stored as SHA-1 hashes of the first 10 characters of the password converted to lowercase.

## **12. NetEase**

Date: October 2015

Impact: 235 million user accounts

Details: NetEase is a provider of mailbox services through the likes of 163.com and 126.com. It was reported in that email addresses and plaintext passwords of some 235 million accounts from NetEase customers were being sold by a dark web marketplace vendor known as DoubleFlag. The same vendor was also selling information taken from other Chinese giants such as Tencent’s QQ.com, Sina Corporation and Sohu, Inc. NetEase has reportedly denied any breach. HaveIBeenPwned lists this breach as “unverified.”

## **13. Sina Weibo**

Date: March 2020

Impact: 538 million accounts

Details: With over 500 million users, Sina Weibo is China’s answer to Twitter. However, in March 2020 it was reported that the real names, site usernames, gender, location, and -- for 172 million users -- phone numbers had been posted for sale on dark web markets. Passwords were not included, which may indicate why the data was available for just ¥1,799 (\$250).

Weibo acknowledged the data for sale was from the company, but claimed the data was obtained by matching contacts against its address book API. It also said that since doesn't store passwords in plaintext, users should have nothing to worry about. This, however, doesn't tally as some of the information being offered such as location data, isn't available via the API. The social media giant said it had notified authorities about the incident and China's Cyber Security Administration of the Ministry of Industry and Information Technology said it is investigating.

#### **14. Yahoo**

Date: 2013-14

Impact: 3 billion user accounts

Details: Yahoo announced in September 2016 that in 2014 it had been the victim of what would be the biggest data breach in history. The attackers, which the company believed were "state-sponsored actors," compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users. Yahoo claimed that most of the compromised passwords were hashed.

Then in December 2016, Yahoo disclosed another breach from 2013 by a different attacker that compromised the names, dates of birth, email addresses and passwords, and security questions and answers of 1 billion user accounts. Yahoo revised that estimate in October 2017 to include all of its 3 billion user accounts.

The timing of the original breach announcement was bad, as Yahoo was in the process of being acquired by Verizon, which eventually paid \$4.48 billion for Yahoo's core internet business. The breaches knocked an estimated \$350 million off the value of the company.

#### **15. Zynga**

Date: September 2019

Impact: 218 million user accounts

Details: Once a giant of the Facebook gaming scene, Farmville creator Zynga is still one the biggest players in the mobile game space with millions of players worldwide.

In September 2019, a Pakistani hacker who goes by the name Gnosticplayers claimed to have hacked into Zynga's database of Draw Something and Words with Friends players and gained access to the 218 million accounts registered there.

Zynga later confirmed that email addresses, salted SHA-1 hashed passwords, phone numbers, and user IDs for Facebook and Zynga accounts were stolen.

Editor's note: This article, originally published in March 2014, is frequently updated to account for new breaches.

# Data Linking and Profiling

## Data Linking

Data linking is used to bring together information from different sources in order to create a new, richer dataset.

This involves identifying and combining information from corresponding records on each of the different source datasets.

The records in the resulting linked dataset contain some data from each of the source datasets.

Most linking techniques combine records from different datasets if they refer to the same entity. (An entity may be a person, organization, household or even a geographic region.)

However, some linking techniques combine records that refer to a similar, but not necessarily the same, person or organization – this is called *statistical linking*.

Complex software is often required to compare identifiers (such as name and address) on the records in both datasets, to assess whether they refer to the same entity. If the identifiers of the records on the different datasets agree, then the records are linked.

## Why is data linking important?

Linked datasets create opportunities for more complex and expanded policy and research.

On the business front, in New Zealand, the Linked Employer-Employee Data (LEED) links taxation data with business data to provide information such as the employment outcomes of tertiary education and transitions from work to retirement and from benefit to work.

Data linking has the advantage of utilizing information that already exists. Making use of data collections in this way avoids the time and expense of collecting a whole new set of data. It also avoids imposing extra questions on people and organizations when this information already exists.



## **The Data Linking Information Series**

These information sheets provide a broad overview of the main technical aspects of data linking.

The Data Linking Information Series currently comprises:

- What is data linking?
- [Preparing for linking](#)
- [Deterministic linking and linkage keys](#)
- [Probabilistic linking](#)
- [Linked data quality](#)

## **What are the main ways to link datasets?**

There are a number of different approaches to data linking.

Usually, the most straightforward way is to use a unique identifier (such as a tax file number) present on both files, in order to identify the links between the records on each dataset. This is sometimes referred to as ‘deterministic’ or ‘exact’ linking because the unique identifiers on the records either match or they do not – there is no uncertainty.

Where a unique identifier is not available, or is not of sufficient quality or completeness to be relied on alone, an alternative approach is to construct a linkage key, which acts as a proxy for the unique identifier. This key (or code) is created using identifiable information, such as name and address, available on both datasets.

Linkage keys can help to preserve privacy because the key replaces name and address, thereby reducing the chance of identification.

Probabilistic linking is another option for linking where a unique identifier is not available. Probabilistic linking is based on a calculation of the likelihood that a pair of records (one drawn from each dataset) refers to the same person/organisation.

Complex methods and sophisticated data linking software are used to achieve high-quality results.

## **Protecting privacy and confidentiality of a linked dataset**

Datasets that contain identifiable information need to be handled with care to protect the identity of a person or organisation.

There is an increased risk of identification of an individual/business/organisation when two datasets are linked.

Even if identification is protected (such as by removing name and address) in the original datasets, the result of the linking may provide a combination of characteristics which leads to spontaneous recognition of the identity of a person or organisation (e.g., local area school data showing a cardiac specialist who is the mother of six).

To minimise this risk, data linking should only be conducted in a safe and effective environment ensuring that the methods used are fit-for-purpose.

Confidentiality and statistical disclosure techniques are available to manage the privacy risks that can be associated with data linking

If a data linking project involves Commonwealth datasets and is for statistical and research purposes the project should comply with the High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes and the supporting governance and institutional arrangements.

# Data Profiling

## I. Approaches to the issue

There are three approaches to thinking about online data collection:

- 1. A consumerist model:** A consumerist model focuses on adequate notice to a consumer that online profiling is occurring, and requires consent before information about the surfer's online behavior can be collected.

Debates within the consumerist model take place over how much notice is required (general notice vs. detailed notice on every page [hypertext link to dashing signals]) and whether "consent" may be *general* ("if you use our web page you impliedly agree that we may collect data about you") or *specific* (consumers required to give explicit consent each time they log on). Regardless of whether a consumerist model requires strong or weak notice, however, in the end under consumerist model a website can restrict a consumer from access unless the consumer agrees to allow the website to collect data.

- 2. A fundamental rights model:** Under a fundamental rights approach to online profiling, an individual's browsing habits would not be allowed to be negotiated away in such a fashion.

By analogy, Congress has forbade video stores from releasing information about what videos one rents. 18 U.S.C. § 2710 (1999).

The Cable Communications Policy Act of 1984 forbids cable operators and third parties from monitoring the viewing habits of subscribers.

Many libraries forbid the release of borrowing records.

These rules, exemplifying a fundamental rights approach to informational privacy, protect a viewer or borrower regardless of the lender's desire to accumulate and sell such information.

- 3. A "market" model:** A marketplace model (sometimes referred to as "self-regulation") would defer to "the market" to work out the resolution of the tensions.

The assumption behind a marketplace approach is that consumers have the power to negotiate what information they wish to disclose to websites. The model takes as its focus the idea of exchange: a user obtains information from a website, and in “exchange” the website collects data about the user. The market approach assumes that whatever data is disclosed—even unwittingly by consumers—is within the power of the collector to share, sell, or retain. The current system defaults to a market model unless a governmental agency (e.g., the Federal Trade Commission) intervenes.

## II. Definitions

Studies have shown that Americans are increasingly concerned about the protection of their privacy on the Internet.

Many of these concerns are well-founded. The nature of the Internet causes information to pass through dozens of networks and computer systems, each with its own manager capable of capturing and storing online activities.

Additionally, user activities can be monitored by individual websites and Internet Service Providers (ISP) (Privacy in Cyberspace, <http://www.privacyrights.org/fs/fs18-cyb.htm>), vastly increasing the availability of one’s personal information to strangers.

*Data profiling “is the term used to denote the gathering, assembling, and collating of data about individuals in databases which can be used to identify, segregate, categorize and generally make decisions about individuals known to the decision maker only through their computerized profile.”*

[Karl D. Belgum, Who Leads at Half Time?: Three Conflicting Versions of Internet Privacy Policy, 6 RICH.J.L.&TECH. 1, 8 \(Symposium 1999\).](#)

A Federal Trade Commission (“FTC”) survey of online practices in 1998 found that ninety-two percent of the 1,402 websites surveyed collected personal data of some sort. This data most often included name, e-mail address, postal address and phone number, although the scope of data that can be collected is wide. When this data is collected in databases, it is often “mined” for information deemed useful to the data collector. Data mining can be used to construct personal data profiles for a variety of purposes. In most circumstances, it is used for targeted marketing. In rare circumstances, however, it can be used for negative

purposes, such as blackmail. [A. Michael Froomkin, The Death of Privacy?, 52 STAN. L. REV. 1461, 1469 \(Symposium 2000\).](#)

Even without the benefit of high-tech equipment, it is possible for website administrators to glean information from a user's click stream – the “aggregation of electronic information generated as a web user communicates with other computers and networks over the Internet. [Adam White Scoville, Clear Signatures, Obscure Signs, 17 CARDOZO ARTS & ENT. L.J. 345, 364 \(1999\).](#)

Often, cookies – “data files created on [users] own computer hard drives when [they] visit a web site [that] contains[s] unique tracking numbers that can be read by the web site,” are used to facilitate data profiling and mining. [Ann Bartow, Our Data, Ourselves: Privacy, Propertization, and Gender, 34 U.S.F.L. REV. 633, 678 \(2000\).](#)

Another device often used to track user's behavior is a “*web beacon*” (*sometimes called a web bug*), which is a miniscule, pixel-sized identifier buried in the software on a page a user views.

According to the Privacy Foundation, A Web bug is a graphic on a Web page or in an e-mail message designed to monitor who is reading the page or message. Web bugs are often invisible because they are typically only 1-by-1 pixels in size. In many cases, Web bugs are placed on Web pages by third parties interested in collecting data about visitors to those pages.

[http://www.bugnosis.org/faq.html#web bug basics](http://www.bugnosis.org/faq.html#web%20bug%20basics)

### **III. The Players**

Entities using data profiling practices can be categorized roughly into two groupings - *private corporations and the government*.

In turn, private companies that profile online use are typically either the website itself (e.g., CNN.com) or a third party advertiser (e.g., Doubleclick). Access to data mines is of great use to the government in that the government “gains powerful investigative tools allowing it to plot the movements, actions, and financial activities of suspects.” [Froomkin 52 STAN. L. REV. 1461.](#)

Furthermore, the government gains the capability to document criminal activities to be used in the prosecution of such suspects. One positive example of

governmental use of data profiling is in the fight to combat credit card fraud in purchases over the Internet. [Scoville 17 CARDOZO ARTS & ENT. L.J. 345 at 364.](#)

However, significant privacy concerns surround when the government ought to be granted access to data mines, both those generated by governmental bodies and those mines created by private entities.

Private corporations, such as individual websites and Internet Service Providers, collect data for their own benefit. Due to technological advances, mining of data has seen a significant reduction in cost, leading to an entire industry dedicated to selling consumer data, particularly to interested marketers. Because private corporations often contract with outside firms to handle their data profiling, companies such as Acxiom (<http://www.acxiom.com>) have come to “[hold] personal and financial information about almost every United States, United Kingdom, and Australian consumer.” [Froomkin 52 STAN. L. REV. 1461 at 1474.](#)

One of the key issues concerning cyberspace data profiling is the extent to which it is different from offline data profiling. For years, catalog companies and others have “mined” data contained in consumer responses to surveys, direct marketing, or purchases. Is Online Data Profiling categorically different from the offline profiling that consumers have accepted for years? If so, those who argue that cyberspace profiling is unique need to explain why it is problematic in that context even if acceptable in the offline context.

#### **IV. Current data profiling practices**

##### *A. Practices of private companies*

Currently, data profiling practices allow companies to obtain useful data through both voluntary disclosure of information and involuntary extraction of information through click stream data.

*Voluntary information* is disclosed by consumers through registration pages, user surveys, online contests, application forms, and transaction documents. For instance, the use of credit cards in online purchasing allows collection of data about a person’s finances, buying habits, etc. Off-line, cash purchasing provides for a certain sense of anonymity. But even off-line, the establishment of loyalty and rewards programs allows for important data to be collected about consumers.

*Involuntary* extraction of click stream data occurs when technology such as cookies, web bugs, and other means track a user's e-mail address, the type of browser being used, the type of computer from which the site is being viewed, and the site from which the user arrived. Additional information that can be extracted includes the geographical location of a user and a user's recent history of page views. These practices allow a company to gain significant information about specific consumers who have not indicated any desire to establish a relationship with the company, thus introducing crucial privacy concerns.

As one can see, therefore, some websites collect personally identifiable information, and other websites collect data about a user which may or may not be personally identifiable. Those that collect personally identifiable information can obtain this information in one of several ways:

(1) The user signs up or otherwise identifies herself to the website (say, through a purchase or by signing up for a sweepstakes);

(2) The user hasn't identified herself to Website X, but has identified herself to Website Y, and Website Y maintains a data-sharing relationship with the first Website;

(3) The user has downloaded software that automatically "reports" back to a website information about the user's online or offline click stream behavior;

(4) The user has a unique IP address [the numerical address to which information is sent on your computer] that can be traced to the particular user.

(5) The user doesn't identify himself to Website Z for several years, but Website Z has dropped a cookie onto the user's computer. Years later, the user purchases something from the website Z. Website Z can back link to the user's prior surfing behavior.

Take for example the fictional website *travel.com*, which hypothetically sells discount airline tickets. Before a prospective buyer is even allowed to browse the offerings on the site, the consumer is required to register. This voluntary disclosure of information might include such seemingly benign pieces of data as name, email address, and possibly the willingness of the consumer to accept emails from the company. After registration, the user may run a few searches looking for discounted airfare to specific cities on specific dates. The user may eventually decide to purchase an airline ticket from Chicago to Cancun, Mexico during the month of January. The consumer may be asked to enter her

age before being allowed to purchase the ticket and then may purchase the ticket use a credit card.

On the back-end of these consumer transactions, the website acquires and stores a significant amount of information about the consumer. After registration, the site is likely to drop a cookie to be stored on the user's hard drive. Information is then gleaned from a user's click stream and the eventual transaction.

When similar information is collected from a number of consumers, the company can "mine" its databases, looking for consumers in a certain age range, for example 17-23, who either purchased tickets to fly to warm climates during typical "winter break periods" or completed searches for fares that met the criterion. If these consumers re-visit the site, then perhaps banner ads for certain products, such as beach ware, will be shown to these repeat visitors, who are recognized by looking for the cookie dropped on their hard-drive during the first visit. For consumers who asked to be sent emails, perhaps emails will be sent with certain specials that the particular type of consumer will may be likely to find interesting.

Therefore, through both voluntary disclosure of information and information "warehoused", or stored, by tracking the user's click stream and transactions, travel.com's data profiling capabilities were used to provide advertising and marketing that was more highly targeted than was ever available before the Internet. This example is quite typical of data profiling practices used every day on the Internet to better target advertising and market individually to consumers.

A major concern of internet users is what happen to their transactional data (or web surfing data) once they have left a website. Many websites are vague on this point (perhaps with reason), and the fear of many users is that their data will be sold to marketers to be combined with many other data sources. *Marketers* certainly have an interest in developing comprehensive user profiles about internet surfers. Such profiles might include detailed information about their interests, tastes, preferences, purchases, work and employment history, salary, and so on. Because such data has no inherent expiration, there's no reason to think it might not be retained for decades.



### *B. Governmental use of data profiling*

“According to a report prepared for the European Parliament, the United States and its allies maintain a massive worldwide spying apparatus capable of capturing all forms of electronic communications. Known as ‘Echelon,’ the network can ‘access, intercept and process every important modern form of communications, with few exceptions [Froomkin 52 STAN. L. REV. 1461](#). The report does not, however, give any insight into current uses of such information.

### **IV. How “mined” data will be used in the future**

With respect to the potential for monitoring one’s activity on the Internet, targeted advertising is only the beginning. Data profiling is only in its infancy, and given the rapidly accelerating growth of developments in the field, data mining could soon “transform modern life in all industrialized countries.” [Froomkin 52 STAN. L. REV. 1461](#).

For instance, one controversial outlet yet to be fully utilized is a unique numerical identifier embedded in each *Intel Pentium III chip*. If exploited, unique identifiers such as those on the processor and also found in certain Microsoft software, would allow a computer to be tracked anywhere in the world, unaffected by changes in application usage.

### **V. Pros and Cons of Data Profiling for Consumers**

It has often been suggested that practices such as data profiling can infringe on users’ privacy. Recently, news organizations have reported on employers’ use of data profiles, abstracted through use of an internal network, in monitoring, or “spying” on their employees. Data profiling has also gotten a negative rap because it can contribute to spam, or unwanted email usually sent to bulk lists of people.

Certainly, the anonymity that a user may have taken for granted in surfing the Internet five years ago, should no longer be viewed as so. On the contrary, for some, just knowing that their activities are being recorded may have a chilling effect on their use of the Internet. One 1999 Forrester report found that “[t]o this day, Web users -- regardless of age, gender, or income -- worry that the information they share online will produce unsolicited spam or telemarketing calls. Even worse, they worry that information they share could come back to haunt them, ultimately harming their relationships, employment, or insurance eligibility.”

Data profiling may also raise consumer privacy concerns to the extent that consumers lose consent privileges over their personal information. Internet users ordinarily cannot control who has access to data mines, or to whom information about them is sold. Additionally, there is no assurance that information collected about consumers is accurate or even kept up to date.

## **VI. How consumers can protect themselves**

The information in this category is fairly specific, in terms of what commands to execute, etc. The general idea is that you can program most browsers, now, to not accept cookies, which helps to guard privacy. However, some websites will not work if the browser setting has been chosen to reject cookies. Alternately, consumers can take advantage of encryption software which may help to some extent, and researching the reputation of sites and programs is always a good idea. Regardless, the basic assumption should always be that the Internet is not a private or anonymous environment and that, unless convinced otherwise by reliable sources, consumers should act with this information in mind.

## **VII. Regulation and Legislation**

Early attempts at enforcing the privacy of Internet users were framed in terms of the tort of invasion of privacy. When it became clear that the traditional tort, for a number of reasons, would not suffice to protect the privacy of consumers in terms of information that was gathered about them without their knowledge or consent, piecemeal attempts at legislation were born.

Today, a handful of federal statutes cover such specific areas as video rental records, student loan information, drivers' license information, and credit reporting (in the Fair Credit Reporting Act 15 U.S.C. §§ 1681-1681s (1999)).

While the Clinton administration succeeded in defining Fair Information Handling Practices in terms of nine privacy principles, and in passing the Children's Online Privacy Protection Act, intense debates linger about how privacy related to data profiling should be protected in the future.

### **A. Self-regulation**

Some attempts have already been made by the industry to show that it is capable of alleviating privacy concerns that result from data profiling practices, on its own. For instance, consumers may recognize that the "TRUSTe" logo has

appeared on many of the more prominent (and even less prominent) websites, recently.

TRUSTe (<http://www.truste.com>) is a company that promotes the privacy principles approved by the U.S. Department of Commerce, FTC, and industry organizations:

1. Adoption and implementation of a privacy policy,
2. Notice and disclosure,
3. Choice and consent, and
4. Data security and quality and access.

In order to receive a “trustmark,” companies must agree to comply with ongoing TRUSTe oversight and consumer resolution procedures. The success and impact the program will have is not yet evident.

There have been and continue to be other attempts at self-regulation to protect data, in particular. For instance, many transactional websites purchase secure “keys” to ensure that information passed to and from their website is encrypted and protected from interception by others. “Firewalls” are also used to protect data.

However, the problem with data profiling is not necessarily that of data getting into the wrong hands, although that is one problem that these measures do help to alleviate. Instead, the problem is the perfectly legal practices of obtaining information about consumers and using it in ways to which they do not consent. To this end, under the current default rules, self-regulation will likely only help protect privacy of consumers if it is worth it to consumers to pay more for privacy than it costs for businesses to respect their privacy. With no data, this would be difficult to assess, but as long as ecommerce continues to grow and consumers do not stop making purchases due to privacy concerns, it would seem that the only incentive for the industry to self-regulate would be to stop the government from stepping in. Interestingly, the same 1999 Forrester Report mentioned above, found that half of consumers were ready to call on the government to regulate online privacy.

### *B. Market Approach*

Some would argue that regulating cyberspace privacy is not necessary. If consumers really cared about privacy, some would say that they would force the industry to provide it. On the other hand, if their personal data were treated as

their property, consumers could promote the development of markets in personal data.

The difficulty with a market approach lies in the fact that it assumes the answer to the question being posed. We are asking whether cyberspace privacy should be protected under one or another legal regime, but the market approach assumes that personal information is freely collectible. The market approach assumes that the current default rule regarding personal information (i.e., that it is freely collectable and alienable by a website to others) is the correct result.

Naturally, if the current default rule is to your advantage you might seek a “market” approach. But there is nothing inherent or “natural” in such an approach any more than it is “natural” that those in possession of your healthcare records are forbidden from releasing them generally to the public. We have rules preventing the release of your medical records (e.g., tort rules holding providers liable for their release; statutes requiring careful treatment of medical records), and these collection and disclosure rules developed over time and with due consideration for the privacy and efficiency interests at stake. There is therefore no reason why one should not review from the ground up reasons for and against calling clickstream data “private” and protectable.

Finally, though proponents of market approach suggest that consumers can renegotiate the terms of their cyberspace dealings, in actuality users are disorganized and individually have exactly no power to affect the collection of data about themselves. Under the “market approach,” a great deal of personal data has already been commodified and is already a part of the public domain subject to purchase, sale and barter by the collectors of that data. Particularly with information that is abstracted involuntarily through a user’s clickstream, a user has little control over who has access to it. It seems bizarre to suggest that cyberspace users have the power to affect (or should organize in this way to affect) the sale and distribution of the data already collected.

A “market” approach, therefore, inevitably defaults to whatever data collection and distribution practice the collector believes will maximize the collector’s revenues. Under the market approach favored by the datacollectors, the argument over “privacy” is over before it begins. The collector, in short, retains the power “to control the acquisition, disclosure, and use--of [your] personal information.” [Jerry Kang, Information Privacy In Cyberspace Transactions, 50 Stanford Law Review 1193, 1203 \(April 1998\).](#)

### *C. Mandatory State Regulation*

Mandatory regulation might be advocated because consumers fear that profit-maximizing marketeers will control their personal information. Mandatory regulation could take any number of forms.

The strongest form, advocated by Professor Jerry Kang, would outright ban retention of cyberspace transactional information after the transaction is complete without an individual's consent. Jerry Kang, *Information Privacy In Cyberspace Transactions*, 50 Stanford Law Review 1193, 1291-93 (April 1998)([section 5 \(b\) of his proposed statute](#)). While Kang's proposed statute does not explicitly address online profiling of nontransactional behavior, the rationale for doing so would seem to be even stronger than the case for banning profiling of consented transactions. Kang's perspective, supported by many online privacy organizations and privacy experts, reflects a fundamental rights approach to online profiling.

A consumerist model, in contrast, would focus on reforming online profiling in an effort to preserve the market in third party accumulation and sale of individuals' private information. Such reform efforts might focus on appropriate notice to consumers that their personal information is being compiled, and require some form of consent to such profiling. A related problem concerns the modification of an online site's privacy policy.

#### 1. Reforming "Notice"

Several different reform possibilities suggest themselves. First, some effort at standardization of the different levels of privacy protection might be undertaken. Presently each website maintains its own privacy policy. These policies vary from vague and cursory to detailed. Because a full understanding of online privacy collection and distribution practices require a fuller understanding of the collection technologies (e.g., cookies, web beacons, IP addresses, browser format) consumers may very well not understand what these privacy policies mean. In addition, many websites disclose to users that they collect certain information, but to learn this the reader must click through to the policy and read and understand several paragraphs.

Some privacy advocates see this as an unrealistic burden: surfers who are concerned about privacy are unlikely to review and analyze the policy of each

website they visit. One possible solution to this dilemma would be to standardize, say, five different levels of online privacy protection. Standardized privacy policies could range from highly protective (“we collect and retain nothing about you beyond the particular transaction”) to the least protective (“whatever you do on our site is monitored and added to our database and sold to third party marketers who amass as much information about you as possible”) would at a minimum assist consumers in making judgments.

Moreover, most websites draft their “privacy policy” with a view towards presenting collection and control of a user’s surfing behavior in the most favorable light. Even those policies that appear to reflect weak privacy protections for their users emphasize that they are concerned about the user’s privacy. For example, the Gap website states that:

*Gap.com values its customers and respects their privacy. We collect customer information in an effort to improve your shopping experience and to communicate with you about our products, services, contests, and promotions. Gap.com recognizes that it must maintain and use customer information responsibly.*

[http://www.gap.com/asp/cs\\_security.asp#3](http://www.gap.com/asp/cs_security.asp#3) (last visited February 25, 2002)

Gap.com goes on to describe in a vague way that it collects information based on a customer’s online behavior:

We collect information (such as your name, email address, mailing address, and phone and credit card numbers) that you provide when you place an order, save your information with us or participate in a contest, promotion or survey. We maintain a record of your product interests and your purchases online and in our stores. We may acquire customer names, email addresses and mailing addresses for select mailings from third parties. [http://www.gap.com/asp/cs\\_security.asp#3](http://www.gap.com/asp/cs_security.asp#3) (last visited February 25, 2002)

From a casual reading of the paragraph, one might conclude that whatever information Gap.com collects is connected to a particular purchase. However, the giveaway in the above paragraph is the tagline that “we maintain a record of your product interests.” This language might have been designed by Gap.com to encompass online profiling without purchases, and if so perhaps Gap.com assumes that it has satisfied its duty to notify customers that it is profiling their online behavior. Since the language is vague, the careful reader can only

guess. However, in this context vagueness in a particular notice about privacy can only serve to obscure what a website is actually doing. If Gap.com is not collecting information about a user's non-purchasing surfing behavior, its lawyers certainly know how to say that clearly.

In admirable contrast to Gap, Amazon.com provides those who read far enough a straight-forward list of the types of information it "automatically" collects from those who visit its website:

Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet; login; e-mail address; password; computer and connection information such as browser type and version, operating system, and platform; purchase history; the full Uniform Resource Locators (URL) clickstream to, through, and from our Web site, including date and time; cookie number; products you viewed or searched for; zShops you visited; your Auction history, and phone number used to call our 800 number.

<http://www.amazon.com/exec/obidos/tg/browse/-/468496/102-1997690-1291327#auto> (last visited February 25, 2002)

In contrast to Gap.com, which may, so far as the reader can tell, also collect such data, Amazon at least particularizes for readers what sorts of information is being gathered, recorded, and stored. To Amazon's credit, it candidly tells the user that every mouse click generated while on its site is being recorded and stored for future purposes.

Even in this context, does the fact that a website is collecting data about users with every mouse click require more prominent notice than that typically contained in privacy policies buried in a website? For example, if one truly wanted to provide notice, one could place a blinking icon at the bottom of every page that explicitly informed users that data was being collected. For example:



*We are collecting  
your mouseclicks!*

In sum, even the consumerist reformers of online profiling must address how much notice must be given, when must it be given, at what level of particularity must it be given, and how detailed must the site describe who will have access to the data.

## 2. Reforming “Consent”

Many privacy advocates continue to be frustrated that consumers realistically have no choice when confronting a website that collects personal data. They argue that a more explicit consent should be sought. Should an explicit approach to notification of users be required? Like the blinking icon (above), a website might be required to obtain explicit consent from a user that it would retain and store any personal information.

A strong consumerist model might require websites to obtain your explicit consent before collecting data. An ironclad consumerist model would require your explicit consent to collect your data without any consequences if you refuse the request. At present, most websites that collect data for their own purposes assert that they use it to benefit their customers. Should websites that collect information that they will sell to other businesses be required to ask consumers’ *specific permission* on every occasion before doing so? For example:

*We would like to collect  
and sell to  
other businesses data  
about your use of our  
site.  
May we? **Yes/No***

## 3. Changing Privacy Policies

A final thorny arena concerns when a website wishes to change its privacy policy. Websites naturally wish to be able to change their privacy policies at will, and many do so regularly. This raises two different types of problems for a consumerist model of reform. First, do regular visitors to a website have an interest in being advised when a privacy policy is changed? Second, may data collected



under one policy be used for a purpose beyond that originally stated in the earlier policy? Both of these issues are troubling for the consumerist model, for change unsettles ongoing relationships, and even surfers who once checked a site's privacy policy may be chagrined later to learn that the policy changed in some unnoticed way.

## **Types of data profiling**

While all applications of data profiling involve organizing and collecting information about a database, there are also three specific types of data profiling.

***Structure discovery-*** This focuses on the formatting of the data, making sure everything is uniform and consistent. It also uses basic statistical analysis to return information about the validity of the data.

***Content discovery-*** This process assesses the quality of individual pieces of data. For example, ambiguous, incomplete and null values are identified.

***Relationship discovery-*** This detects connections, similarities, differences and associations between data sources.

## **Privacy policies and their specifications**

A **Privacy Policy** is a legal agreement designed to let visitors to your website or users of your app know what personal information you gather about them, how you use this information and how you keep it safe.

A Privacy Policy for a website or app generally covers:

- The **types of information collected** by the website or app
- The **purpose** of this data collection
- Data storage, security and access
- Details of data **transfers**
- Affiliated websites or organizations
- Cookies

## **Do I need a Privacy Policy?**

If you collect any sort of personal information about visitors to your website or users of your app then **you legally need to have a Privacy Policy**.

**Examples of personal information** your website or app might collect include:

- Names
- Dates of birth
- Email addresses
- Billing/ shipping addresses
- Phone numbers
- Bank details
- Social security numbers

There are **4 important reasons** why you need to have a Privacy Policy if you collect personal information.

### **1. It's required by law**

This is the most important reason to have a Privacy Policy on your website or app. Privacy laws in most countries dictate that website owners and app developers need to make a Privacy Policy available to their users.

For example, in the US the **California Online Privacy Protection Act (CalOPPA)** instructs that all commercial websites and apps that collect and maintain personally identifiable information from California residents must have a Privacy Policy:

#### **Who does CalOPPA apply to?**

CalOPPA applies to any person or entity that owns or operates a commercial website or online service that "collects and maintains personally identifiable information from a consumer residing in California who uses or visits" said website or online service. CalOPPA does not apply to Internet service providers or similar entities that transmit or store personally identifiable information for a third party.

In 2012, the California Attorney General's Office specifically applied CalOPPA to mobile applications for smartphones and tablets that collect personally identifiable information. Hundreds of apps providers were notified that they were in violation of CalOPPA, and they were given 30 days to submit compliance plans or face fines of up to \$2,500 for each time their app was downloaded.

If you are based in the US, but not in California, it's still important that your website or app complies with CalOPPA because a resident of California could still access and use your services.

Similar privacy laws exist in Canada, Australia and across Europe. The next section looks at privacy laws by country in more detail.

## **2. It's often required by third-party services**

You also need a Privacy Policy if you use third-party services that track users for analytics **or** display targeted advertising.

Even *seemingly* anonymous data, like what web browser someone uses, is considered personally identifiable information because it can be used in combination with another type of data to identify an individual.

For example, if you use Google Analytics **you need a Privacy Policy** because it uses cookies to collect information about your website's visitors.

[Google Analytics'](#) Terms of Service dictate that any business who uses their services must:

*"post a Privacy Policy and that Privacy Policy must provide notice of your use of cookies, identifiers for mobile devices (e.g., Android Advertising Identifier or Advertising Identifier for iOS) or similar technology to collect data. You must disclose the use of Google Analytics, and how it collects and processes data."*

Similarly, you will need to have a Privacy Policy in place if you develop apps across platforms that collect user data.

[Facebook's Platform Policy](#) states that you must:

*"Provide a publicly available and easily accessible privacy policy that explains what data you are collecting and how you will use that data."*

Equally, if you submit an app to Apple's App Store, the [App Store Review Guidelines](#) states that you are expected to have a Privacy Policy visible to your users:

*"All apps must include a link to their privacy policy in the App Store Connect metadata field and within the app in an easily accessible manner."*

## **Privacy policy languages,**

Most Privacy Policies are published in English. While this may not seem like the most considerate approach in non-English speaking countries, it is not required for Privacy Policies to be available in a country's native language.

## **Within privacy laws**

Current privacy laws require clear outlines of information practices and conspicuous links to Privacy Policies. Users should be able to find them easily either on a website or through an app download platform. Many websites also provide a checkbox and link at sign-up to assure acceptance of the terms as affirmative consent is becoming preferable to passive acceptance.

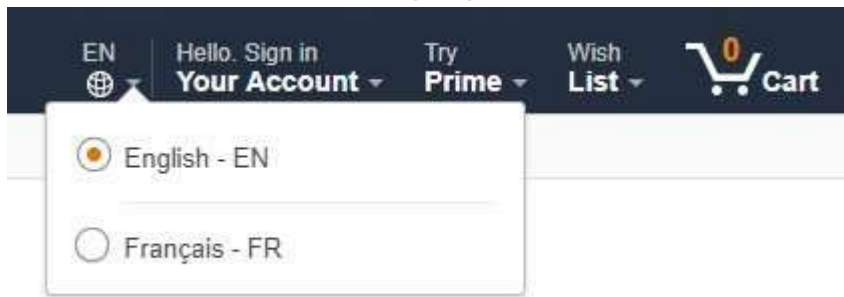
The one issue not addressed in these laws is language. Even though privacy laws may not include this issue, there are laws that can affect how you present your agreements online.

### **Official Languages Act**

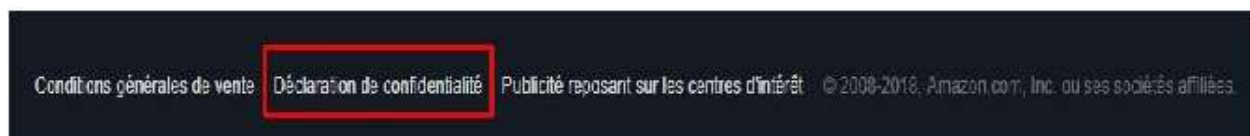
The [Official Languages Act](#) is a Canadian law requiring food labels, websites, and literature to be available in both English and French. That is due to the fact that both are official languages in Canada.

As a result, users have the option to choose their language when they visit a Canadian website. This is done through a drop down menu in a prominent part of the page.

[Amazon Canada](#) offers a good example of how to handle language choices. When the user visits the page, there is a small icon next to the sign in button that allows the user to choose their language:



Once switched to French, there is still a link to the Privacy Policy at the bottom, which is also in French:



The link takes the user to the French version of the Privacy Policy. If the user decides she would rather review legal terms in English, the option to switch languages is available at the top of the page:

The screenshot shows the Amazon.ca website header with the logo and navigation links. A red arrow points to the text "Would you like to see this page in English? Click here." in the top navigation bar. Below the header, the page title is "Déclaration de confidentialité Amazon.ca" and the content includes a search bar, a sidebar with navigation links, and the main text of the privacy policy.

amazon.ca  
Essayez Prime

Toutes ▾

Voire adresse de livraison: États-Unis

Parcourir par Boutiques ▾

Chez vous Nos bonnes affaires Cartes-cadeaux Vendre Aide

Would you like to see this page in English? [Click here.](#)

## Aide et service à la clientèle

Rechercher dans le

↳ Toutes les rubriques d'aide

### Sécurité et confidentialité

- Demander des renseignements
- Cà publique PGP
- Signaler un problème de sécurité
- Courriels d'Amazon.ca
- Votre charte des droits Amazon.ca
- Normes de la chaîne d'approvisionnement
- Déclaration de confidentialité Amazon.ca**
- Conditions d'utilisation
- Choisir un mot de passe fort
- Protéger votre système
- Navigateurs compatibles

Sécurité et confidentialité

## Déclaration de confidentialité Amazon.ca

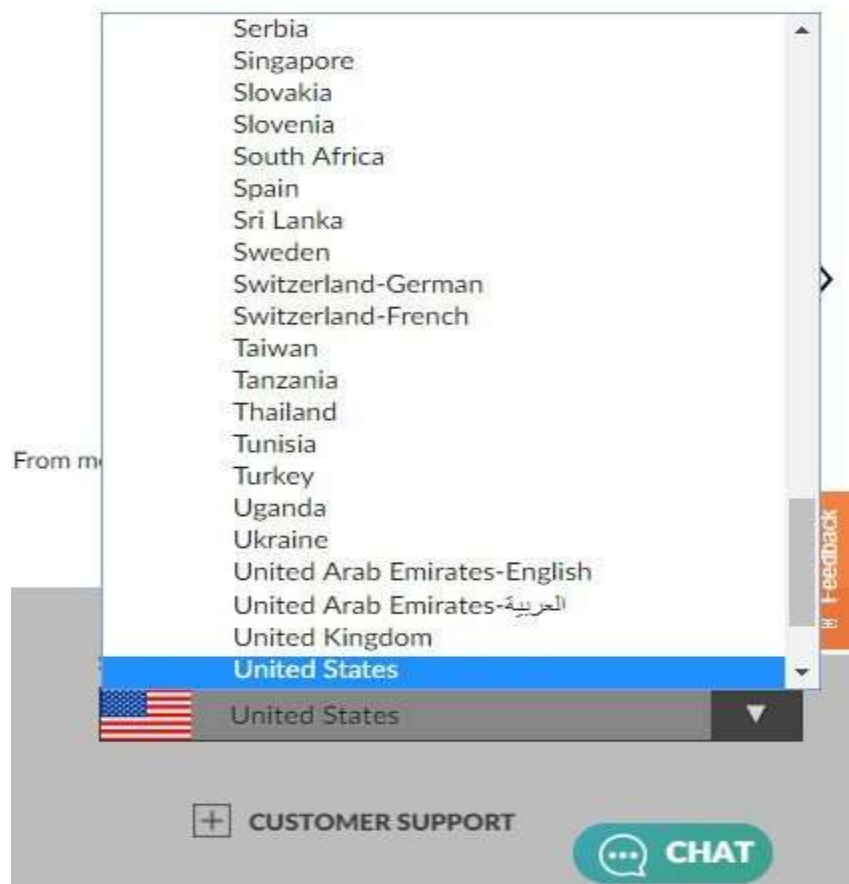
Dernière mise à jour : le 18 août 2017 ([Cliquez ici](#) pour voir les modifications.)

À Amazon.ca, nous contrôlons rigoureusement la façon dont les renseignements personnels que vous nous fournissez sont utilisés et communiqués, et nous sommes sensibles à la confiance que vous placez en nous à cet égard. La présente Déclaration de confidentialité énonce notre politique de protection des renseignements personnels. **En utilisant le site Amazon.ca, vous acceptez de vous conformer aux pratiques décrites dans la présente Déclaration de confidentialité.**

- Quels renseignements personnels Amazon.ca recueille-t-il sur ses clients?
- Les témoins (cookies)
- Es-ce qu'Amazon.ca divulgue les renseignements qu'il reçoit?
- Mes renseignements personnels sont-ils vraiment protégés?
- Les annonceurs tiers et des liens vers d'autres sites Internet
- Quels renseignements puis-je consulter?
- Quels choix me sont offerts?
- Les enfants sont-ils autorisés à utiliser Amazon.ca?
- Conditions d'utilisation, avis et révisions
- Exemples de renseignements recueillis

Other websites may have translation options but typically do not apply them to their legal agreements. Basically, website content on products and company history are translated, but not the Privacy Policy.

[Lenovo](#) maintains headquarters in Beijing, China and Morrisville, North Carolina, US. It sells computer hardware all over the world. As expected, its website offers an option in the footer to change countries and website language:



Once you choose a language, the link to the Privacy Policy becomes available in that language.

Here's what happens when you choose to read the website in Dutch:



Despite the fact that the user is on the Dutch language site for Lenovo, the Privacy Policy is still presented in English:

## Lenovo Privacy Statement

[Website Privacy](#) / [Product Privacy](#)

Lenovo recognizes that privacy is of great importance to individuals everywhere—our customers, website visitors, product users... everyone. This is why the responsible use and protection of personal and other information under our care is a core Lenovo value. To learn more about our privacy practices, please click any of the links below. If you have any further questions or concerns, please feel free to reach us at [privacy@lenovo.com](mailto:privacy@lenovo.com).

The privacy statement was last updated on 08/28/2017.



This seems to be an exception rather than the rule at Lenovo. However, it happens because of a simple reason--maintaining agreements in all languages is not required.

Regardless of requirements, translating your agreements into as many languages as possible may be a good business practice.

### **Consider Your User Base**

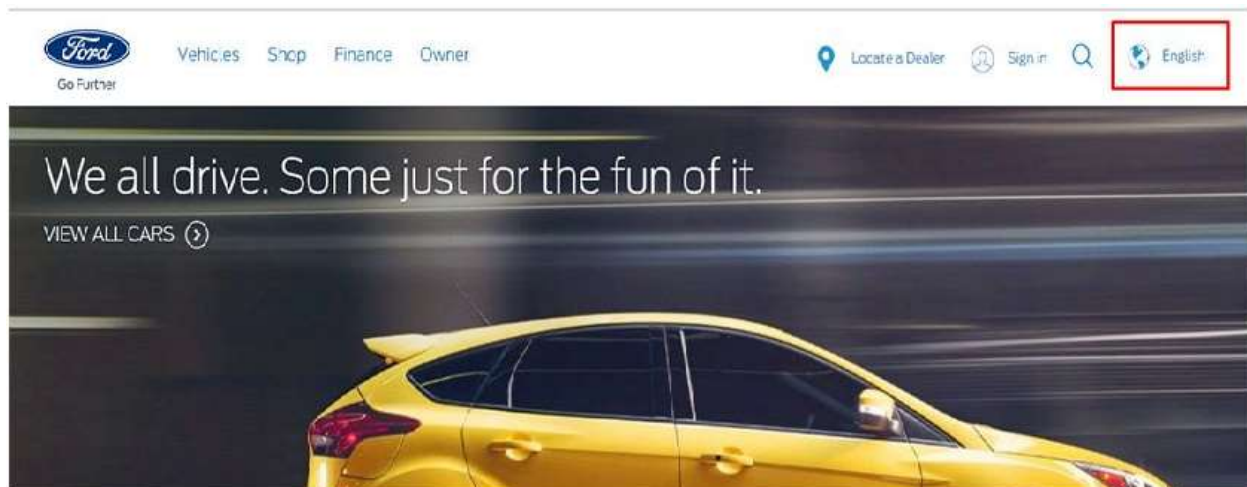
If your customer base includes different cultures and languages, it is likely a good idea to offer your Privacy Policy in those languages. Many companies provide this service not just due to their international reach, but also because their local base happens to be diverse.

In the U.S., English is the dominant language with [237.8 million speakers](#). Spanish is also a common spoken language taking second place to English with 40.5 million speakers. This trend is likely to grow as immigrants from Mexico and Central America move into the American north and southwest creating communities where Spanish is the primary language.

American businesses are aware of this. Spanish speakers purchase cars, seek professional services, and secure medical care. Many businesses focus on hiring bilingual employees so they can better communicate with this clientele.

[Ford Motor Co.](#) is among the companies noticing this demographic shift. Dealerships seek Spanish-speaking sales representatives and its website caters to this population.

As a result, when you visit Ford's website, it offers an option in the footer to change website's language:



Clicking this box lets a user choose between reading the website in English or Spanish:



Once switched to Spanish, the Privacy Policy link is available in that language:



This takes you to a Spanish version of the Privacy Policy.

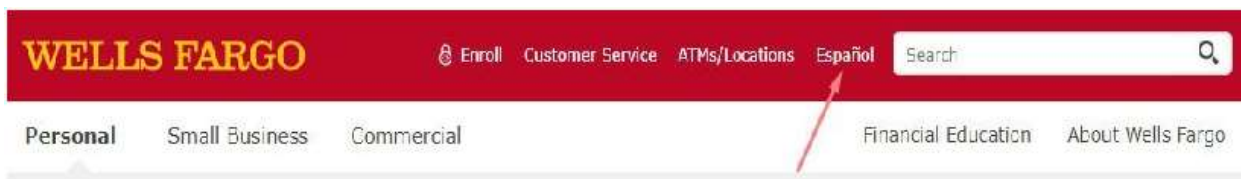


Ford is not alone in this practice.

[Wells Fargo](#) is a national banking chain that is headquartered in California--where many Spanish-speaking immigrants live.

It offers an option in the header to switch the website to the Spanish language:





When switched to Spanish, here's the link to the Privacy Policy in the footer:



And here's the Privacy Policy in Spanish:

## Privacidad, seguridad y asuntos legales

Imprima Comparta



### Cómo prevenir el fraude y el robo de identidad



Obtenga más información >

#### Privacidad, seguridad y asuntos legales

Durante hace más de 160 años, Wells Fargo ha estado dedicado a la seguridad de las cuentas y de la información, y nuestra misión sigue más firme que nunca. Obtenga información sobre cómo le protegemos, y sobre cómo puede protegerse identificando y denunciando actividad fraudulenta.

#### Avisos y políticas de privacidad

Comprenda cómo utilizamos y protegemos la información personal.

- ➔ Aviso de privacidad del consumidor de los EE.UU. de Wells Fargo
- ➔ Política de privacidad digital y de cookies
- ➔ Política de protección del Número del Seguro Social
- ➔ Aviso de privacidad de Wells Fargo Financial National Bank (PDF) 
- ➔ Aviso de privacidad de Dillard's de Wells Fargo Bank, N.A. (PDF) 
- ➔ Aviso sobre información médica
- ➔ Avisos de privacidad de Wells Fargo International

#### Denuncie el fraude

Transacciones sospechosas con tarjeta de débito/ATM

1-877-727-2932

Transacciones sospechosas con tarjeta de crédito

1-800-642-4720 (marque 9 para español)

Transacciones sospechosas por Internet

1-866-867-5568 (en inglés)

Companies based in European nations also realize the value of offering websites in multiple languages.

[Croatia Airlines](#) offers a number of options for website languages in its header:



Once the user chooses a language, there is a link to the Privacy Policy in that language in the footer. This example is the Spanish version:



When the user follows the link, they find the Privacy Policy in their chosen language:

» Declaración de privacidad

## Declaración de privacidad

www.croatiaairlines.com/es está comprometida a proteger su privacidad y la tecnología de desarrollo que le brinda la experiencia en línea más potente y segura. Esta Declaración de Privacidad está relacionada con el sitio Web de www.croatiaairlines.com/es y abarca la recolección de datos y su uso. Al utilizar el sitio www.croatiaairlines.com/es, Usted acepta las prácticas utilizadas en relación a los datos que se describen en esta declaración.

### Recolección de su Información Personal

www.croatiaairlines.com/es recolecta información de identificación personal, como su dirección de correo electrónico (e-mail), nombre, dirección del trabajo o de su casa, o su número telefónico. www.croatiaairlines.com/es también recaba información demográfica anónima, en el sentido que no es aplicable sólo a Usted, como por ejemplo el código postal, edad, sexo, preferencias, intereses y favoritos.

También existe información acerca del hardware y software de su computador personal, que se recaba automáticamente por www.croatiaairlines.com/es. Esta información puede incluir: su dirección IP, tipo de explorador de Internet usado, nombres de dominio, tiempos de acceso y direcciones de sitios Web que hacen referencia a éste. Esta información es utilizada por www.croatiaairlines.com/es para la operación del servicio, para mantener la calidad del servicio prestado y para brindar estadísticas generales acerca del uso del sitio www.croatiaairlines.com/es.

It can take a lot of effort to translate online agreements. Hiring a translator who specializes in legal terms is not easy or cheap.

While it is always good to accommodate your customers, assess thoroughly whether it is absolutely necessary.

## **Privacy in different domains- medical, financial:**

Privacy, as distinct from confidentiality, is viewed as the *right of the individual*

*client or patient* to be let alone and to make decisions about how personal information is shared (Brodnik, 2012). Even though the U.S. Constitution does not specify a “right to privacy”, privacy rights with respect to individual healthcare decisions and health information have been outlined in court decisions, in federal and state statutes, accrediting organization guidelines and professional codes of ethics.

The top-of-mind example is the federal HIPAA Privacy Rule, establishing national standards for health information privacy protection and defining “protected health information” (HHSa, 2003, p. 1). A stated purpose of the HIPAA Privacy Rule “...is to define and limit the circumstances in which an individual’s protected health information may be used or disclosed...”(HHSa, 2003, p. 4).

Established pursuant to the broader Health Insurance Portability and Accountability Act of 1996 (HIPAA), as described by the U.S. Department of Health and Human Services (HHS), the Privacy Rule, “...strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing” (HHSa, 2003, p. 1). Individuals are provided some elements of control, such as the right to access their own health information in most cases and the right to request amendment of inaccurate health information (HHSa, 2003, pp. 12-13). However, in that attempt to strike a balance, the Rule provides numerous exceptions to use and disclosure of protected health information without patient authorization, including for treatment, payment, health organization operations and for certain public health activities (HHSa, 2003, pp. 4-7).

### **Cybercrime: Examples and Mini-Cases**

#### **OFFICIAL WEBSITE OF MAHARASTRA GOVERNMENT HACKED**

MUMBAI, 20 September 2007 — IT experts were trying yesterday to restore the official website of the government of Maharashtra, which was hacked in the early hours of Tuesday.

Rakesh Maria, joint commissioner of police, said that the state’s IT officials lodged a formal complaint with the Cyber Crime Branch police on Tuesday. He added that the hackers would be tracked down. Yesterday the website, <http://www.maharashtragovernment.in>, remained blocked.

Deputy Chief Minister and Home Minister R.R. Patil confirmed that the Maharashtra government website had been hacked. He added that the state government would seek the help of IT and the Cyber Crime Branch to investigate the hacking.

“We have taken a serious view of this hacking, and if need be the government would even go further and seek the help of private IT experts. Discussions are in progress between the officials of the IT Department and experts,” Patil added.

The state government website contains detailed information about government departments, circulars, reports, and several other topics. IT experts working on restoring the website told Arab News that they fear that the hackers may have destroyed all of the website’s contents.

According to sources, the hackers may be from Washington. IT experts said that the hackers had identified themselves as “Hackers Cool Al-Jazeera” and claimed they were based in Saudi Arabia. They added that this might be a red herring to throw investigators off their trail.

According to a senior official from the state government’s IT department, the official website has been affected by viruses on several occasions in the past, but was never hacked. The official added that the website had no firewall.

Indian Banks Lose Millions of Rupees,

Bank heists have not gone out of fashion just yet, both as a cinematic trope, and also as a shortcut to riches. A total of 972 such incidents were reported in 2017-18, roughly three every day, according to data collated by the Reserve Bank of India (RBI).

The information was furnished by the Minister of State (MoS) for Finance in the Lok Sabha in response to a question regarding the number of ATM robberies, and the safety of financial outposts in the country. The data presented in the lower house of parliament includes incidents of robbery, dacoity, burglary, and theft directed at financial institutions in the last three years.

The banking sector lost a total of Rs 168.74 crore to organised crime directed at ATMs in the past three years. This includes figures for the first quarter of FY19. Between April and June 2018, 261 incidents were reported, entailing a loss of Rs 18.85 crore to banks.

**2001 Parliament attack: When terror struck India's temple of democracy**

On 13 December, 2001, Pakistan-sponsored terror struck India's temple of democracy. Five terrorists infiltrated Parliament complex and tried to enter the Parliament building. They entered the Parliament complex in a car that had a forged Union home ministry pass. Both the houses of Parliament were adjourned 40 minutes before they intruded the complex. But, many MPs, ministers, officials and other staffs were inside the Parliament complex at that time. Terrorists moved towards gate No. 12 to enter the building, but they were stopped by the Parliament security. Terrorists opened fire and a gunfight between terrorists and security personnel lasted for over 30 minutes. Luckily terrorists could not enter the parliament and all the five terrorists were killed in the gunfight. Eight security personnel and a gardener lost their life in the incident. Investigation revealed that the terrorists belonged to Pak-based Jaish-e-Mohammad and Lashkar-e-Taiba. Their Indian associates Afzal Guru, Shaukat Hussain, SAR Geelani and Navjot Sandhu were arrested. All of them were tried in a court. Nation pays tribute to the Bravehearts with gratitude every year on December 13.

### **Pune City Police Bust Nigerian Racket**

The city police on Friday busted an international phishing racket with the arrest of six persons, including five Nigerian nationals, who allegedly hacked bank accounts of more than 100 people.

Two laptops, three internet data cards, six ATM cards, six mobile phones, 20 SIM cards, a car and three Nigerian passports were recovered from the arrested persons -- Sunny Uche Uzoma (35), Michael Animba (27), Onyegbuna Udochukwu (35), Nwazonobi Amaeze Obed (40) and Tinuola Yussuf Olatunji (37), all Nigerians along with Prabhu Jayadeep Patvari (23) from Mumbai.

The gang was also wanted by the police in Delhi, Mumbai, Tamil Nadu and Gujarat, Hyderabad Police Commissioner Anurag Sharma told media persons here on Friday.

Explaining the modus operandi, Mr. Sharma said accomplices of the Nigerians in India would come to a city and enter into a rental agreement with property owners. Using fake documents they would apply for a landline phone connection and after getting the phone bill, they would use it to open a savings bank accounts.

The gang members would later apply for a trade licence from the Labour Department. After getting the trade licence, they would open current accounts. With the help of their associates in India, the gang would send emails containing fake bank pages to lakhs of people. “Many fell into the trap and sent their online banking details,” Mr. Sharma said.

The gang then used to access the bank details of customers. The Nigerians would target accounts having huge cash and pass on the details to their accomplices in India who would transfer the funds using fake ID to the accounts created earlier fraudulently.

After deducting their commission, the accomplices here would transfer the remaining amount to the Nigerian nationals who would buy clothes and return to their country by ship. “Connivance of a few officials coupled with superficial checking by bank officials, labour department and service providers is leading to this problem,” the Commissioner said.

The accused, Prabhu Jayadeep Patvari, managed to secure 154 SIM cards in three months and the gang was also able to open 38 accounts fraudulently in the city.

The police also managed to stop money transfer of Rs.61 lakh by alerting a nationalised bank but the gang managed to withdraw Rs.5 lakh using a cheque.

The fraud came to light when branch manager of Sanghvi Corporation, Kailash Nath Seth, complained to the police that Rs.5 lakh was fraudulently transferred to a Kanpur PNB account. He gave two phone numbers from which an unidentified person claiming to be a bank employee took a password from him. With this information, the police first caught Patvari and later the five others.

### **e-mail spoofing instances**

Email spoofing is the fabrication of an email header in the hopes of duping the recipient into thinking the email originated from someone or somewhere other than the intended source. Because core email protocols do not have a built-in method of



authentication, it is commonplace for spam and phishing emails to use said spoofing to trick the recipient into trusting the origin of the message.

The ultimate goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation. Although the spoofed messages are usually just a nuisance requiring little action besides removal, the more malicious varieties can cause significant problems, and sometimes pose a real security threat.

As an example, a spoofed email may purport to be from a well-known retail business, asking the recipient to provide personal information like a password or credit card number. The fake email might even ask the recipient to click on a link offering a limited time deal, which is actually just a link to download and install malware on the recipient's device.

One type of phishing – used in business email compromise – involves spoofing emails from the CEO or CFO of a company who works with suppliers in foreign countries, requesting that wire transfers to the supplier be sent to a different payment location.

#### How Email Spoofing Works

Email spoofing is possible because the Simple Mail Transfer Protocol (SMTP) does not provide a mechanism for address authentication. Although email address authentication protocols and mechanisms have been developed to combat email spoofing, adoption of those mechanisms has been slow.

#### Reasons for Email Spoofing

Although most well-known for phishing purposes, there are actually several reasons for spoofing sender addresses. These reasons can include:

- Hiding the sender's true identity – though if this is the only goal, it can be achieved more easily by registering anonymous mail addresses.
- Avoiding spam block lists. If a sender is spamming, they are bound to be block listed quickly. A simple solution to this problem is to switch email addresses.
- Pretending to be someone the recipient knows, in order to, for example, ask for sensitive information or access to personal assets.
- Pretending to be from a business the recipient has a relationship with, as means of getting ahold of bank login details or other personal data.
- Tarnishing the image of the assumed sender, a character attack that places the so-called sender in a bad light.



- Sending messages in someone's name can also be used to commit identity theft, for example, by requesting information from the victims financial or healthcare accounts.

### **Email Spoofing Protections**

Since the email protocol SMTP (Simple Mail Transfer Protocol) lacks authentication, it has historically been easy to spoof a sender address. As a result, most email providers have become experts at detecting and alerting users to spam, rather than rejecting it altogether. But several frameworks have been developed to allow authentication of incoming messages:

- SPF (Sender Policy Framework): This checks whether a certain IP is authorized to send mail from a given domain. SPF may lead to false positives, and still requires the receiving server to do the work of checking an SPF record, and validating the email sender.
- DKIM (Domain Key Identified Mail): This method uses a pair of cryptographic keys that are used to sign outgoing messages, and validate incoming messages. However, because DKIM is only used to sign specific pieces of a message, the message can be forwarded without breaking the validity of the signature. This is technique is referred to as a "replay attack".
- DMARC (Domain-Based Message Authentication, Reporting, and Conformance): This method gives a sender the option to let the receiver know whether its email is protected by SPF or DKIM, and what actions to take when dealing with mail that fails authentication. DMARC is not yet widely used.

### **How Emails are spoofed**

The easiest way to spoof mails is for the attacker finds a mail server with an open SMTP (Simple Mail Transfer Protocol) port. SMTP lacks any authentication so servers that are poorly configured have no protection against prospective cyber criminals. It's also the case that there is nothing stopping a determined attackers from setting up their own email servers. This is very common in In cases of CEO/CFO fraud. Attackers will register domains easily confused for the company they are impersonating, where the email is originating from – e.g. "@exarnple.com" instead of "@example.com". Depending on the formatting of the email, it might be extremely difficult for a regular user to notice the difference. Although email spoofing is effective in forging an email address, the IP address of the computer sending the mail can generally be identified from the "Received:"

line in the email header. This is frequently due to an innocent third party becoming infected by malware, which hijacks the system and sends emails without the owner even realizing it.

### **Why Email Spoofing is Important**

To prevent becoming a victim of email spoofing, it is important to keep anti-malware software up to date, and to be wary of tactics used in social engineering. When unsure of the validity of an email, contacting the sender directly, especially if sharing private or financial information, can help to avoid an attack.