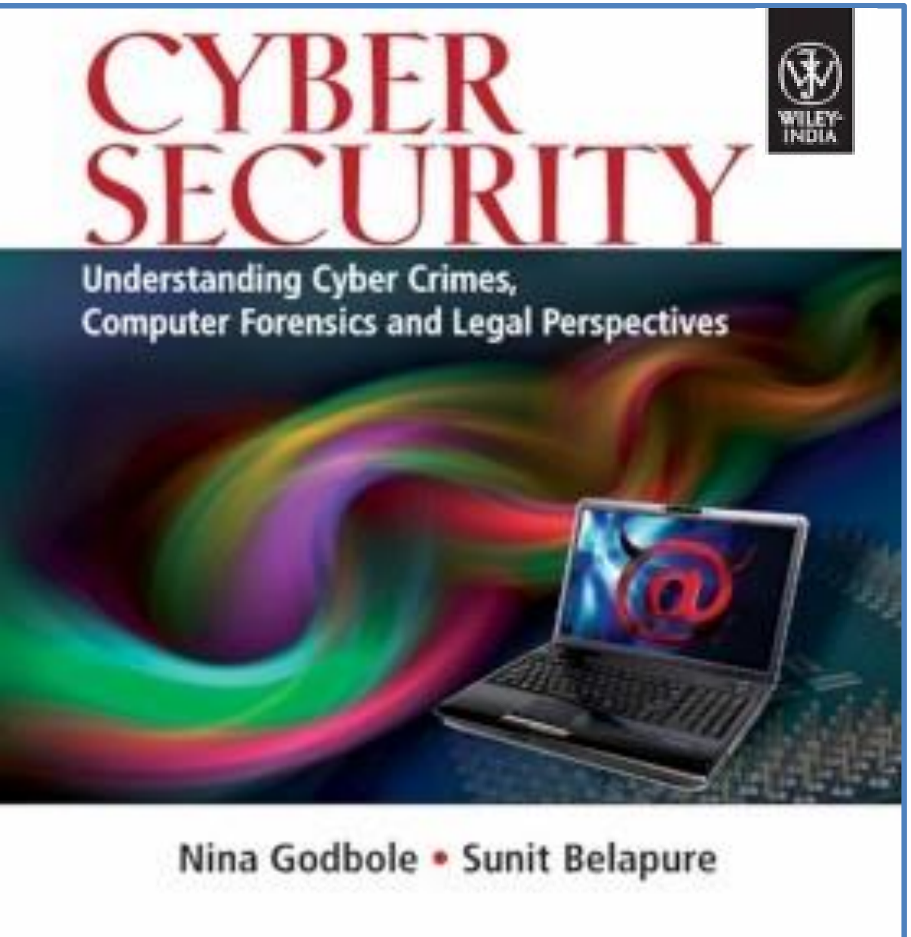
Unit-2

Lesson-3

Cyberoffenses: How Criminals Plan Them

Chapter 2
Cyberoffenses: How Criminals Plan Them


CYBER SECURITY
Understanding Cyber Crimes, Computer Forensics and Legal Perspectives
WILEY-INDIA
Nina Godbole • Sunit Belapure

Introduction

In today’s world of Internet and computer networks, a criminal activity can be carried out across national borders with “false sense of anonymity”.

An attacker would look to exploit the vulnerabilities in the networks such as:

1. Inadequate border protection (border as in the sense of network periphery);
2. remote access servers (RASs) with weak access controls;
3. application servers with well-known exploits;
4. misconfigured systems and systems with default configurations.

Categories of Cybercrime

Cybercrime can be categorized based on the following:
1. The target of the crime and
2. whether the crime occurs as a single event or as a series of events.

The target of the crime

1. Crimes targeted at individuals
2. Crimes targeted at property
3. Crimes targeted at organizations
4. Single event of cybercrime
5. Series of events

How Criminals Plan the Attacks

1. Reconnaissance (information gathering) is the first phase and is treated as passive attacks.
2. Scanning and scrutinizing the gathered information for the validity of the information as well as to identify the existing vulnerabilities.
3. Launching an attack (gaining and maintaining the system access).

Reconnaissance

"Reconnaissance" is *an act of reconnoitering – explore, often with the goal of finding something or somebody* (*especially to gain information about an enemy or potential enemy*).

Reconnaissance begins with "*Footprinting*" – this is the preparation toward pre-attack phase

- involves accumulating data about the target's environment and computer architecture to find ways to intrude into that environment.

Passive Attacks

- A passive attack involves gathering information about a target without his/her (individual's or company's) knowledge.
- It is usually done using Internet searches or by Googling an individual or company to gain information.

Active Attacks

- An active attack involves probing the network to discover individual hosts to confirm the information gathered in the passive attack phase.
- It involves the risk of detection and is also called “*Rattling the doorknobs*”or “*Active reconnaissance*.”
- Active reconnaissance can provide confirmation to an attacker about security measures in place.

Scanning and Scrutinizing Gathered Information

The objectives of scanning are:

1. Port scanning: Identify open/close ports and services.

2. Network scanning: Understand IP Addresses and related information about the computer network systems.

3. Vulnerability scanning: Understand the existing weaknesses in the system.

Attack (Gaining and Maintaining the System Access)

After the scanning and enumeration, the attack is launched using the following steps:

1. Crack the password;
2. exploit the privileges;
3. execute the malicious commands/applications;
4. hide the files (if required);
5. cover the tracks – delete the access logs, so that there is no trail illicit activity.

Social Engineering

- It is the “technique to influence” and “persuasion to deceive” people to obtain the information or perform some action.
- Social engineers exploit the natural tendency of a person to trust social engineers’ word, rather than exploiting computer security holes.
- Social engineering involves gaining sensitive information or unauthorized access privileges by building inappropriate trust relationships with insiders.
- The sign of truly successful social engineers is that they receive information without any suspicion.

Classification of Social Engineering

1. *Human-Based Social Engineering*

Human-based social engineering refers to person-to-person interaction to get the required/desired information.

2. *Computer-Based Social Engineering*

Computer-based social engineering refers to an attempt made to get the required/desired information by using computer software/Internet.

Cyberstalking

- It is defined as the use of information and communications technology, particularly the Internet, by an individual or group of individuals to harass another individual, group of individuals, or organization.
- Cyberstalking refers to the use of Internet and/or other electronic communications devices to stalk another person.
- It involves harassing or threatening behavior that an individual will conduct repeatedly.
- As the Internet has become an integral part of our personal and professional lives, cyberstalkers take advantage of ease of communication and an increased access to personal information available with a few mouse clicks or keystrokes.

Types of Stalkers

There are primarily two types of stalkers as listed below:

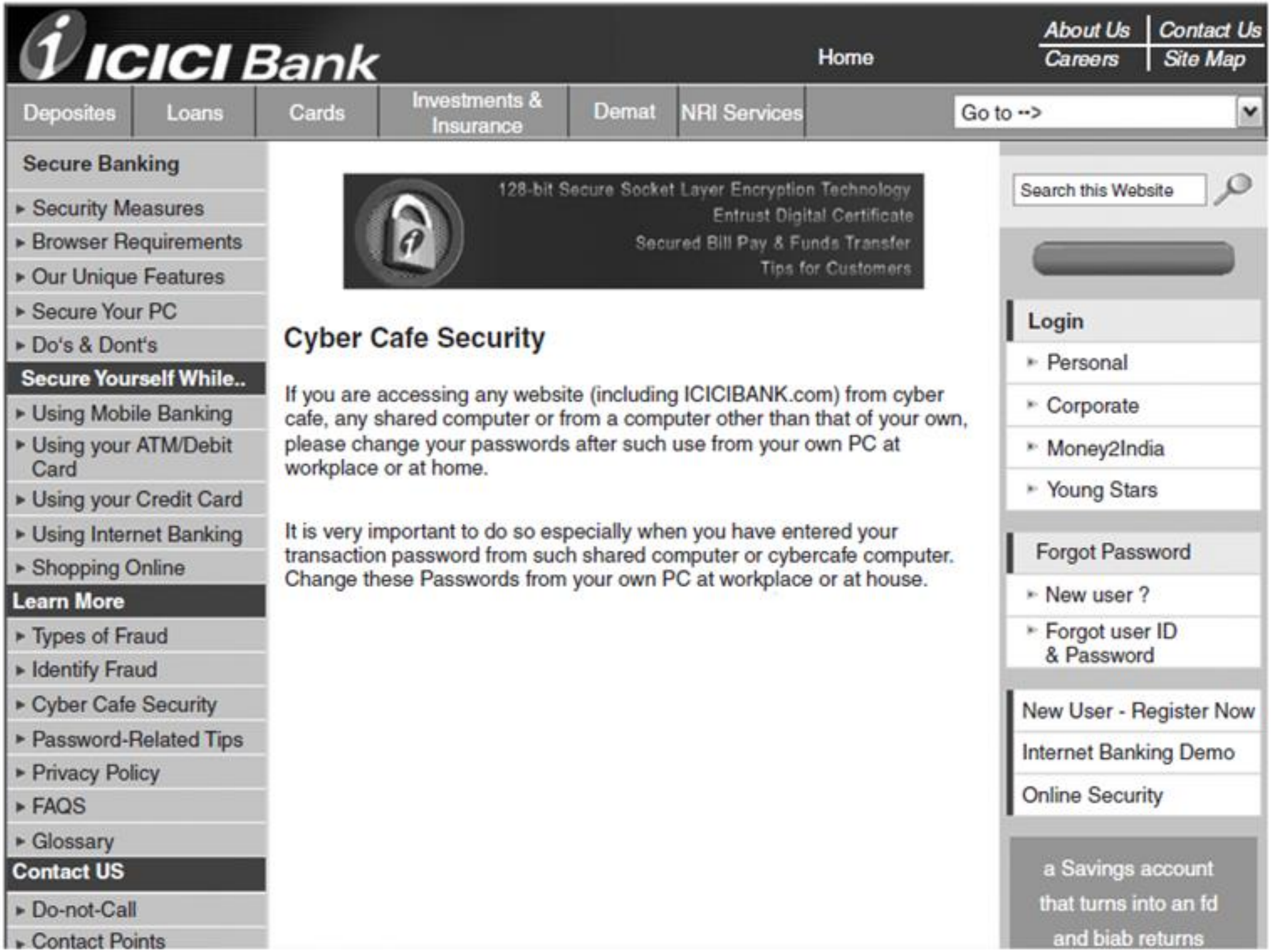
1. **Online stalkers**: They aim to start the interaction with the victim directly with the help of the Internet.
2. **Offline stalkers:** The stalker may begin the attack using traditional methods such as following the victim, watching the daily routine of the victim, etc.

How Stalking Works?

1. Personal information gathering about the victim
2. Establish a contact with victim through telephone/cell phone. Once the contact is established, the stalker may make calls to the victim to threaten/harass.
3. Stalkers will almost always establish a contact with the victims through E-Mail. The stalker may use multiple names while contacting the victim.
4. Some stalkers keep on sending repeated E-Mails asking for various kinds of favors or threaten the victim.
5. The stalker may post the victim's personal information on any website related to illicit services such as sex-workers' services or dating services, posing as if the victim has posted the information and invite the people to call the victim on the given contact details The stalker will use bad and/or offensive/attractive language to invite the interested persons.
6. Whosoever comes across the information, start calling the victim on the given contact details asking for sexual services or relationships.
7. Some stalkers subscribe/register the E-Mail account of the victim to innumerable pornographic and sex sites, because of which victim will start receiving such kind of unsolicited E-Mails.

Cybercafe and Cybercrimes

- Cybercrimes such as stealing of bank passwords and subsequent fraudulent withdrawal of money have also happened through cybercafes.
- Cybercafes have also been used regularly for sending obscene mails to harass people.
- Indian Information Technology Act (ITA) 2000 interprets cybercafes as "network service providers" referred to under the erstwhile Section 79, which imposed on them a responsibility for "due diligence" failing which they would be liable for the offenses committed in their network.

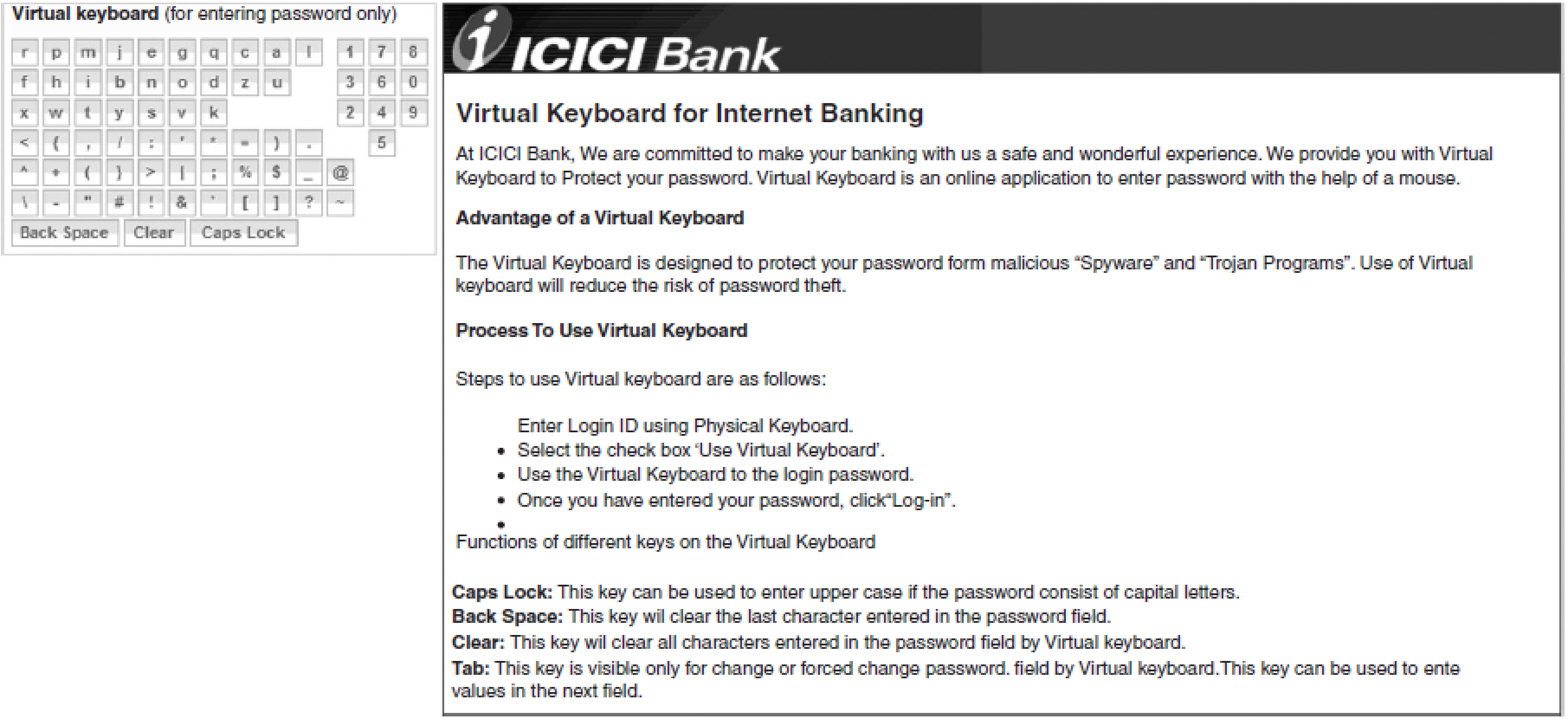


Cyber Cafe Security

If you are accessing any website (including ICICIBANK.com) from cyber cafe, any shared computer or from a computer other than that of your own, please change your passwords after such use from your own PC at workplace or at home.

It is very important to do so especially when you have entered your transaction password from such shared computer or cybercafe computer. Change these Passwords from your own PC at workplace or at house.

Figure 1 Cybercafe security.
Source: http://www.icicibank.com/pfsuser/temp/cybersec.htm (27 June 2009).



Virtual Keyboard for Internet Banking

At ICICI Bank, We are committed to make your banking with us a safe and wonderful experience. We provide you with Virtual Keyboard to Protect your password. Virtual Keyboard is an online application to enter password with the help of a mouse.

Advantage of a Virtual Keyboard

The Virtual Keyboard is designed to protect your password form malicious "Spyware" and "Trojan Programs". Use of Virtual keyboard will reduce the risk of password theft.

Process To Use Virtual Keyboard

Steps to use Virtual keyboard are as follows:

Enter Login ID using Physical Keyboard.

- Select the check box 'Use Virtual Keyboard'.
- Use the Virtual Keyboard to the login password.
- Once you have entered your password, click"Log-in".

Functions of different keys on the Virtual Keyboard

Caps Lock: This key can be used to enter upper case if the password consist of capital letters.
Back Space: This key wil clear the last character entered in the password field.
Clear: This key wil clear all characters entered in the password field by Virtual keyboard.
Tab: This key is visible only for change or forced change password. field by Virtual keyboard.This key can be used to ente values in the next field.

Figure 2 Virtual keyboard.
Source: http://www.icicibank.com/pfsuser/webnews/virtualkeyboad.htm (27 June 2009).

Cybercriminals can either install malicious programs such as keyloggers and/or Spyware or launch an attack on the target.

Here are a few tips for safety and security while using the computer in a cybercafe:

1. Always logout
2. Stay with the computer
3. Clear history and temporary files
4. Be alert
5. Avoid online financial transactions
6. Change passwords
7. Virtual keyboard
8. Security warnings

Botnets: The Fuel for Cybercrime

- A Botnet (also called as zombie network) is a network of computers infected with a malicious program that allows cybercriminals to control the infected machines remotely without the users' knowledge.
- Your computer system maybe a part of a Botnet even though it appears to be operating normally.
- Botnets are often used to conduct a range of activities, from distributing Spam and viruses to conducting denial-of-service (DoS) attacks.

One can ensure following to secure the system:

1. Use antivirus and anti-Spyware software and keep it up-to-date.
2. Set the OS to download and install security patches automatically.
3. Use a firewall to protect the system from hacking attacks while it is connected on the Internet.
4. Disconnect from the Internet when you are away from your computer.
5. Downloading the freeware only from websites that are known and trustworthy
6. Check regularly the folders in the mail box – “sent items” or “outgoing” – for those messages you did not send.
7. Take an immediate action if your system is infected.

Attack Vector

- An “attack vector” is a path or means by which an attacker can gain access to a computer or to a network server to deliver a payload or malicious outcome.
- Attack vectors include viruses, E-Mail attachments, webpages, pop-up windows, instant messages, chat rooms, and deception.
- The most common malicious payloads are viruses, Trojan Horses, worms, and Spyware.
- If an attack vector is thought of as a guided missile, its payload can be compared to the warhead in the tip of the missile.
  - ✓ Payload means the malicious activity that the attack performs.
  - ✓ It is the bits that get delivered to the end-user at the destination.

The attack vectors described here are how most of them are launched:

1. Attack by E-Mail
2. Attachments (and other files)
3. Attack by deception
4. Hackers
5. Heedless guests (attack by webpage)
6. Attack of the worms
7. Malicious macros
8. Foistware (sneakware)
9. Viruses

Cloud Computing

Cloud computing services, while offering considerable benefits and cost savings makes it easier for cybercriminals to attack these systems.

Cloud computing is Internet (“cloud”)-based development and use of computer technology (“ computing”).

A cloud service has three distinct characteristics which differentiate it from traditional hosting:

1. It is sold on demand
2. it is elastic in terms of usage
3. the service is fully managed by the provider.

Advantages of Cloud Computing

Cloud computing has following advantages:

1. Applications and data can be accessed from anywhere at any time.
2. It could bring hardware costs down.
3. Organizations do not have to buy a set of software or software licenses for every employee and the organizations could pay a metered fee to a cloud computing company.
4. Organizations do not have to rent a physical space to store servers and databases. Servers and digital storage devices take up space.
5. Organizations would be able to save money on IT support because organizations will have to ensure about the desktop (i.e., a client) and continuous Internet connectivity instead of servers and other hardware.

The cloud computing services can be either private or public.

- A public cloud sells services to anyone on the Internet.
- A private cloud is like a proprietary network or a data center that supplies the hosted services to a limited number of people.

Types of Services

Services provided by cloud computing are as follows:

1. Infrastructure-as-a-service (IaaS)
2. Platform-as-a-service (PaaS)
3. Software-as-a-service (SaaS)

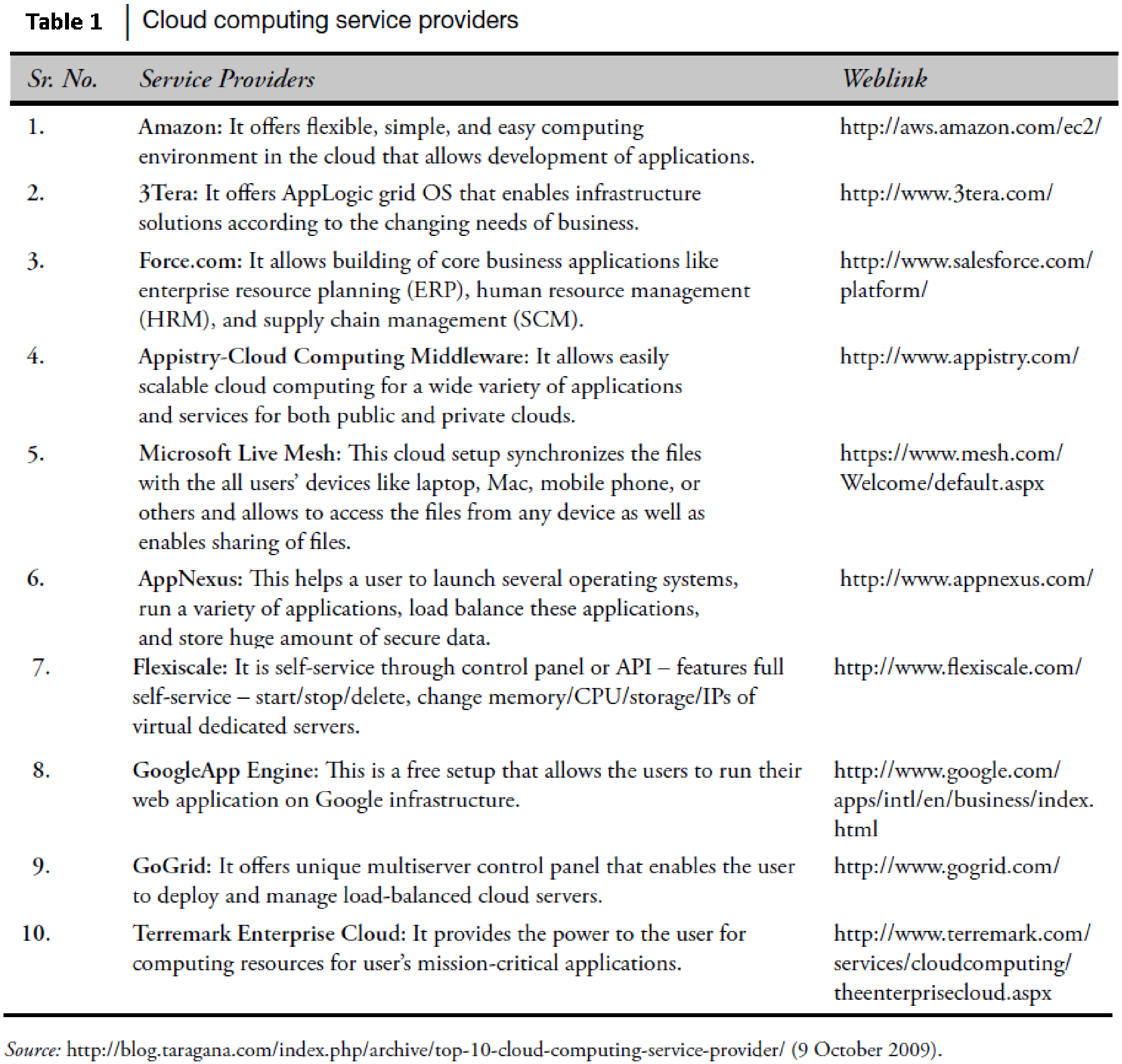


Table 1 | Cloud computing service providers

Sr. No.	*Service Providers*	*Weblink*
1.	**Amazon:** It offers flexible, simple, and easy computing environment in the cloud that allows development of applications.	http://aws.amazon.com/ec2/
2.	**3Tera:** It offers AppLogic grid OS that enables infrastructure solutions according to the changing needs of business.	http://www.3tera.com/
3.	**Force.com:** It allows building of core business applications like enterprise resource planning (ERP), human resource management (HRM), and supply chain management (SCM).	http://www.salesforce.com/platform/
4.	**Appistry-Cloud Computing Middleware:** It allows easily scalable cloud computing for a wide variety of applications and services for both public and private clouds.	http://www.appistry.com/
5.	**Microsoft Live Mesh:** This cloud setup synchronizes the files with the all users' devices like laptop, Mac, mobile phone, or others and allows to access the files from any device as well as enables sharing of files.	https://www.mesh.com/Welcome/default.aspx
6.	**AppNexus:** This helps a user to launch several operating systems, run a variety of applications, load balance these applications, and store huge amount of secure data.	http://www.appnexus.com/
7.	**Flexiscale:** It is self-service through control panel or API – features full self-service – start/stop/delete, change memory/CPU/storage/IPs of virtual dedicated servers.	http://www.flexiscale.com/
8.	**GoogleApp Engine:** This is a free setup that allows the users to run their web application on Google infrastructure.	http://www.google.com/apps/intl/en/business/index.html
9.	**GoGrid:** It offers unique multiserver control panel that enables the user to deploy and manage load-balanced cloud servers.	http://www.gogrid.com/
10.	**Terremark Enterprise Cloud:** It provides the power to the user for computing resources for user's mission-critical applications.	http://www.terremark.com/services/cloudcomputing/theenterprisecloud.aspx

Source: http://blog.taragana.com/index.php/archive/top-10-cloud-computing-service-provider/ (9 October 2009).

Cybercrime and Cloud Computing

Prime area of the risk in cloud computing is protection of user data.
Table 2 shows the major areas of concerns in cloud computing domain.

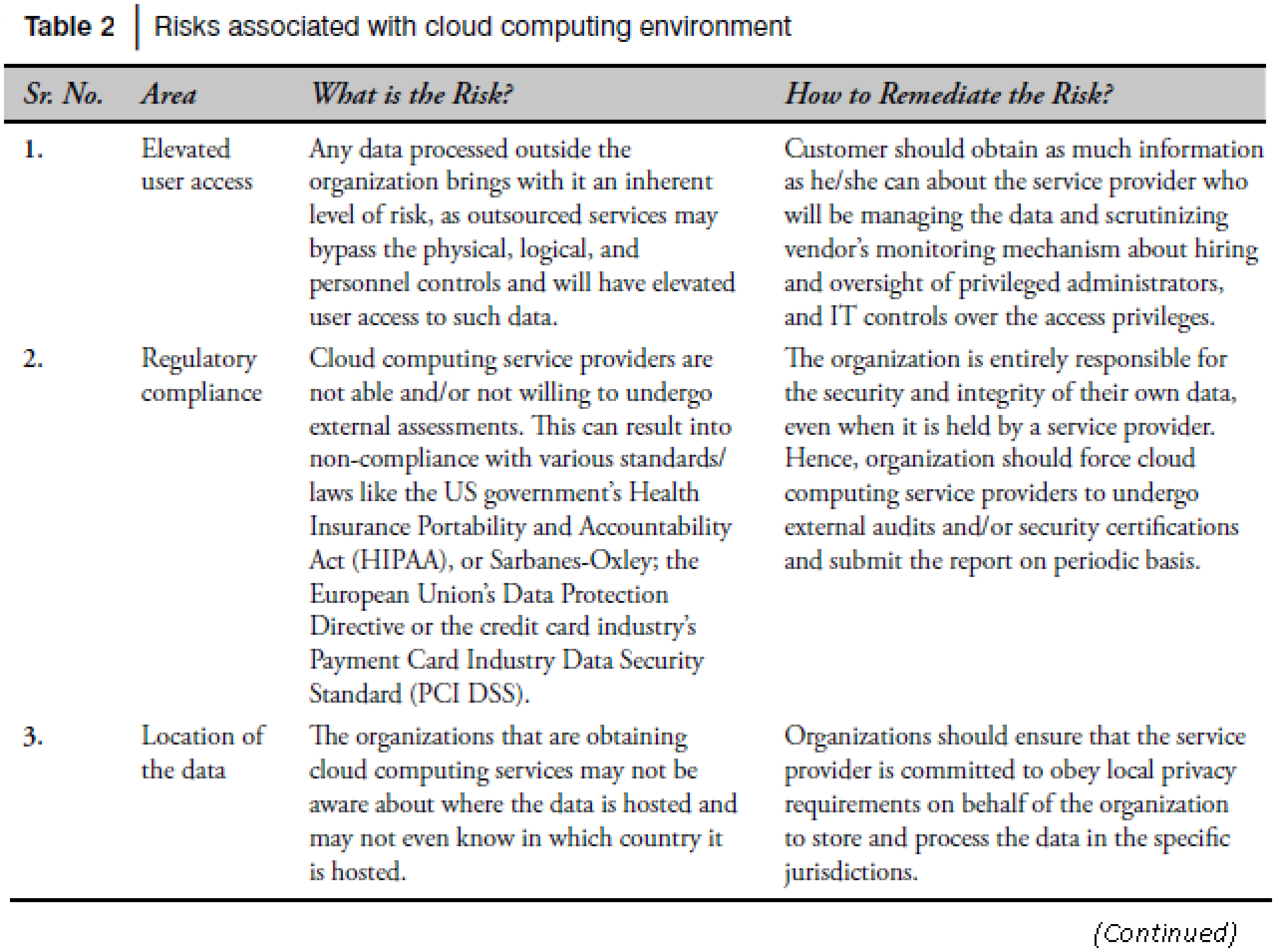
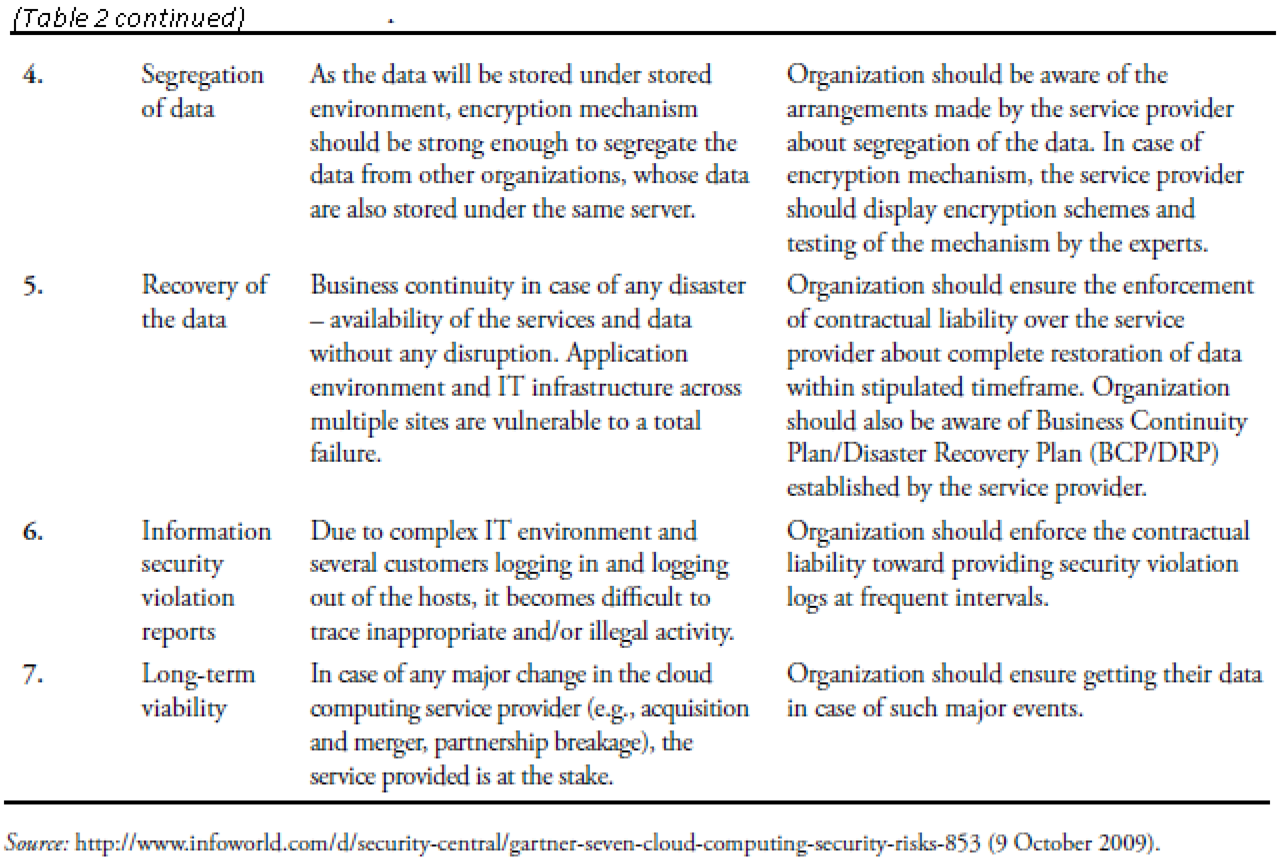


Table 2 | Risks associated with cloud computing environment

Sr. No.	*Area*	*What is the Risk?*	*How to Remediate the Risk?*
1.	Elevated user access	Any data processed outside the organization brings with it an inherent level of risk, as outsourced services may bypass the physical, logical, and personnel controls and will have elevated user access to such data.	Customer should obtain as much information as he/she can about the service provider who will be managing the data and scrutinizing vendor's monitoring mechanism about hiring and oversight of privileged administrators, and IT controls over the access privileges.
2.	Regulatory compliance	Cloud computing service providers are not able and/or not willing to undergo external assessments. This can result into non-compliance with various standards/laws like the US government's Health Insurance Portability and Accountability Act (HIPAA), or Sarbanes-Oxley; the European Union's Data Protection Directive or the credit card industry's Payment Card Industry Data Security Standard (PCI DSS).	The organization is entirely responsible for the security and integrity of their own data, even when it is held by a service provider. Hence, organization should force cloud computing service providers to undergo external audits and/or security certifications and submit the report on periodic basis.
3.	Location of the data	The organizations that are obtaining cloud computing services may not be aware about where the data is hosted and may not even know in which country it is hosted.	Organizations should ensure that the service provider is committed to obey local privacy requirements on behalf of the organization to store and process the data in the specific jurisdictions.

(Continued)



(Table 2 continued)

4.	Segregation of data	As the data will be stored under stored environment, encryption mechanism should be strong enough to segregate the data from other organizations, whose data are also stored under the same server.	Organization should be aware of the arrangements made by the service provider about segregation of the data. In case of encryption mechanism, the service provider should display encryption schemes and testing of the mechanism by the experts.
5.	Recovery of the data	Business continuity in case of any disaster – availability of the services and data without any disruption. Application environment and IT infrastructure across multiple sites are vulnerable to a total failure.	Organization should ensure the enforcement of contractual liability over the service provider about complete restoration of data within stipulated timeframe. Organization should also be aware of Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) established by the service provider.
6.	Information security violation reports	Due to complex IT environment and several customers logging in and logging out of the hosts, it becomes difficult to trace inappropriate and/or illegal activity.	Organization should enforce the contractual liability toward providing security violation logs at frequent intervals.
7.	Long-term viability	In case of any major change in the cloud computing service provider (e.g., acquisition and merger, partnership breakage), the service provided is at the stake.	Organization should ensure getting their data in case of such major events.

Source: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853 (9 October 2009).

Questions

- What are the “mobility types”? Quote day-to-day examples of familiarity that relates to them
- What is botnet? What are the countermeasures to be undertaken to protect the system against botnet?
- What is attack vector? What are the different modes with which attack vectors can be launched?
- What are the Popular types of attacks against 3G mobile networks?
- What kinds of cybersecurity measures an organization should have to take in case of portable storage devices?
- Explain the four risks associated with cloud computing environment related to cybercrime.

Questions

- Define Cyberstalking. How stalking works?
- What is social engineering? Describe the two types of social engineering.
- What is cybercafé? What are the safety and security measures to be adopted while using the computer in a cybercafé?
- Describe the Organizational Policies for the Use of Mobile Hand-Held Devices
- How criminals plan the attacks? Explain passive attacks and active attacks.