**Internet fundamental and Application**

**12/5/2019**

Ishwor Khatiwada

TOPIC: INTRANET

An intranet is a powerful tool for any business, making it easier to share documents and files between users and to work collectively on group projects. Intranet is intended only for organization and its employees, Intranet became a popular way of sharing information and communicating more effectively. Intranet network can provide users with many different functions such as centralized document repository, custom forms and social networking tools.

However, intranets do come with a few drawbacks that must be considered before deployment. An intranet can offer you great efficiency and safety gains, but those gains are made at the cost of flexibility and user freedom.

**MANAGEMENT ISSUES:**

**LOSS OF CONTROL:**  
 One of the major disadvantages is the risk of security to the corporate information resource. The intranet exposes the corpo­rate information resource to the risk of loss of privacy and even unauthorized alteration. The Intranet technology is still quite fragile and the risk of security and privacy of information on Intranet is higher.

**Complexity and costly**

Intranet users often have heavy administrative burden causing additional time waste. Building and implementing an intranet network can be expensive. Depending on how many users you need connected and what type of security measures you want to implement, adding an intranet can demand a significant investment. Moreover, older PCs will need to be upgraded to more easily interact with the network, and users will need to be trained on how to efficiently use the intranet for work-related tasks. All of these factors can increase the total cost of implementation.

**Potential for chaos**

With the increase in productivity that advantages of intranet bring, it will also bring in more and more customer, queries which ultimately increase higher tasks. A number of tasks compared to workers available to meet the demand may not be in proportion, which consequently leads to a pile up of work. This will send the business into chaos as they cannot meet the rapid demand.

**Security Concern**

Unauthorized Access:

Although Intranet software does have security settings, this technology is quite susceptible to being hacked or damaged. There is a chance that data may be stolen and privacy may be violated. This puts your business and its work at quite a risk.  While it is true that the sharing of files and documents between users can boost productivity, it is also true that the sharing of files puts them at greater risk. When several people are working on documents simultaneously, it's easier for those documents to be potentially be deleted or damaged or may be in wrong hands. Moreover, sharing of usernames and passwords can compromise the security of your Company Intranet.

**Denial of Services:**

These attacks are aimed at overwhelming an intranet with data requests, which makes it inoperable.To protect against DDoS attacks, your IT professionals should utilize such tools as firewalls, and load balancers to control the volume of traffic reaching your intranet.

**Packet Sniffing:** Sniffing in general terms refers to investigate something covertly in order to find confidential information From an information security perspective, sniffing refers to tapping the traffic or routing the traffic to a target where it can be captured, analyzed and monitored. Sniffing is usually performed to analyze the network usage, troubleshooting network issues, monitoring the session for development and testing purpose.

**Productivity Concern:**

**Overabundance of information**

Lower productivity:

Set up own web pages: