**Question 1: Bill’s business is already expanding. He thinks that in a few weeks, he will need to hire one or two employees to help him. He knows that each new employee will need their own computer. He is also making the necessary changes so that the new employees will be working in a spare room in Bill’s house. Explain to Bill what networking options he has. Go through each type or configuration of network possible for him, making sure that you explain the pros and cons of each configuration. Finish with your suggestion for the network that he should set up and explain what new hardware will be required to do this.**

* Making internet connection- A solid internet connection is the cornerstone of any small business. A local cable or phone company is always a good start for a ISP( Internet Service Provider). They have the option of DSL(Digital Subscriber Line) and cable connections. There are some pro and cons to both options.

DSL: Pros- You can access both the internet and your phone line at the same time, faster than dial-up, and ability to choose between different connection speeds. Cons- Receives data faster than it sends it, sometimes not available in remote areas, and the farther you are from the provider's central location the slower the transmission.

Cable: Pros- Performance isnt based on distance from the provider's central location and is faster than dial up and most often dsl. Cons- The more people using it at the same time the slower the performance, costs more than DSL, and sometimes not available in remote areas.

* Wifi Networks- It’s always good to have Wi-Fi, so that workers can roam within the office with notebooks or tablets. (Not to mention smartphones—configuring them to use the office Wi-Fi network can help reduce the use of pricey cellular data.) To guard against eavesdropping, just be sure to use WPA2 security with a long, strong passphrase. Better yet, for the utmost in wireless security you can [upgrade to WPA2-Enterprise](http://www.smallbusinesscomputing.com/webmaster/upgrade-to-wpa2-enterprise-wi-fi-security.html). The D-Link DWL-6600AP to your network.
* Small Business Phone Systems- Many ISPs now offer Internet-based office phone systems that provide a full range of advanced business-class features (e.g. auto-attendant, company directory, voicemail to email, etc.) without the need for an on-site PBX and that can be paid for monthly without any large initial outlay—though some ISPs may require a multi-year contract. Even better, these phone systems are generally easily manageable via a Web browser, so routine administration chores (adding/removing extensions and other configuration changes) cost little time and no money. Ooma office offers unlimited calling in the US and Canada for only $19.98 a month.
* Network Printers- A network-connected printer (or multifunction unit with scan, copy, and possibly fax capabilities) is a necessity for almost any office. Almost all printers—even low-end sub $100 models—come with built-in Wi-Fi, but it’s worth it to go upmarket a bit to find models that also include Ethernet connectivity, such as the [HP Officejet 8600 Plus](http://www.smallbusinesscomputing.com/ProductReviews/Hardware/small-business-printer-review-hp-officejet-pro-8600-plus.html). (Ethernet is easier to set up and generally offers a more reliable connection.)

**Question 2: With the possibility of three business computers in his home, and all of his business records possibly vulnerable, this would be a good time to advise Bill on how to set up a routine plan to protect and defend his new network. Provide a list of the five most important concerns for safety and security of the network and the computers in the network. For each concern, specify the action to be taken, and if applicable, what software you recommend be added to the system. Justify each of your recommendations.**

* Weak passwords: 52% of people who use computers do not use secure enough passwords. Avoid using pet names, birthdays, or any personal data. Use a combination of capital and lowercase letters, numbers, & symbols. Make it between 8 to 12 characters long and make habit of changing the password every 90 days.
* Put up a strong firewall: A firewall protects your network by controlling internet traffic coming into and flowing out of your business. Comodo has been voted one of the best free firewalls for a couple of years now.
* Secure your laptops: Because they are portable, laptops are at a higher risk for being lost of stolen than a desktop. Its important to take extra measures to protect your data. Encrypt your laptop. Encryption software changes the way information looks on the hard drive, so that without the correct password, it cant be read.
* Backup regularly: Scheduling regular backups to an external hard drive, or in the cloud, is a painless way to ensure that all your data is stored safely. Servers should be completely backed up weekly. Getting your data compromised is stressful, but having it already backed up is an easy way to avoid any extra issues.
* Educate your employees: Teaching your employees about safe online habits & protective defense is key. Make sure your employees understand how important your company's data is and all the measures they can take to protect it.