The Dangers of a Software Monoculture:

Monoculture is the term that is derived from agriculture. The actual definition of the monoculture is the agricultural practice of producing or growing a single crop or plant species over a wide area and for a large number of consecutive years. In the context of software and computers, monoculture means a group of computers or majority of computers are running on identical software. In present world, more than 80% computers are operated on Microsoft operating system. It indicates Microsoft is the major creator of monoculture in the software world. The prominent issue with a monoculture is that it is vulnerable to the same type of attack. In the context of agriculture if one virus can affect one variety of a crop, there is high probability for the same variety and conditions of crop getting affected. Computers exhibits almost similar behavior. If everyone is using similar OS or similar application or similar protocol to access a network, any security bug or risk is identified in that OS or Software or protocol, a single attack can affect everything. It points out the need heterogeneity in software industry. But the software monoculture suffers from three basic flaws. The first flaw is comparing software monoculture to agriculture monoculture. Whenever there is an active and powerful virus is in action, why not all the computers in the world using same OS are not getting affected? The reason is those computers may be having advanced updated antivirus software. Even two systems might be having same operating system or application software; they might have different antivirus software and different firewalls and different configurations. This is one of the reasons behind why popular viruses did not affect every system. The other reason is the security team capable to develop and deploy the security patches, new antivirus updates and configurations. The second flaw in the monoculture analysis is having heterogeneity factor. Achieving this factor needs large amount of money. Suppose a IT company have got few systems running on Windows, few other on Linux and other variants like sun Solaris and UNIX variants; it costs more to hire experts in each domain. It might cost twice or thrice if we have different types of operating systems. A single operating system locked down by experts is far more

secure than two operating systems configured by sysadmins who aren't so expert. The third flaw is that we may get a limited amount of diversity using two operating systems from three different manufacturers. In monoculture context, two is little better than one. In worst case, diverse network is less secure as it is easily affected to the attacks against one of it heterogeneous components. Some degree of monoculture is necessary in computer networks. Most of the times we communicate others in same terminology and trying to be different may not give much security. In conclusion, we can say monoculture is dangerous thing and is important. But analyzing all the factors such as time, cost and efforts to ensure our current infrastructure is more than important.

When to Change Passwords:

Changing password at regular time intervals is the one of the most discussed thing in the security domain. Most of the people feel inconvenience with their employer or bank password expiration policy; finally they change password and ends up with forgetting it or writing it somewhere in the most of cases. The downside of a password changing policy is it makes the end user to choose a simple or weak password. So there is need to consider this factor while making password changing policies. There is no need to regularly change the password to personal computer or for low-security accounts. We should change our corporate login password occasionally, and we need to take a good hard look at our friends, relatives, and paparazzi before deciding how often to change our social network website password. It is mandatory to change the password whenever there is any kind of personal issues with people who we have shared our computer or personal accounts. The primary reason to give an authentication credential -- not just a password, but any authentication credential -- an expiration date is to limit the amount of time a lost, stolen, or forged credential can be used by someone else. For example if a Credit card is lost it can be used until it's end date. After that, it's useless.

This becomes less important when the credential contains a biometric, evens a photograph or is verified online. It's much less important for a credit card or passport to have an expiration date now that they're not so much bearer documents as just pointers to a database. If, for example, the credit card database knows when a card is no longer valid, there's no reason to put an expiration date on the card. But the expiration date does mean that a forgery is only good for a limited length of time. Passwords are of same kind like credit card expiration date. If a hacker cracks our password by any means of hacking technique, he can access our accounts as long as the password is valid. If we update password regularly, that will limits the hacker to do more damage. But in most of cases whenever a hacker gets password of a user he directly starts doing damage to our account, in the case of bank account hacker may transfer all the money to his account. In case of social network hacker may delete or post unwanted updates. At these situation changing password regularly won't helps, but it is vital need to change the password instantly after noticing the attack. Someone committing espionage in a private network is more likely to be stealthy. But he's also not likely to rely on the user credential he guessed and stole; he's going to install backdoor access or create his own account. Here again, forcing network users to regularly change their passwords is less important than forcing everyone to change their passwords immediately after the spy is detected and removed, you don't want him getting in again. Finally, there is no reason to change any password that is a key to an encrypted file; just keep the same password as long as we keep the file, unless we suspect it's been compromised. If there is a need to change password for financial related or any personal related logins proper care should be taken to choose a more complex password. To have a strong password it is advised to check the password through online password strength examine websites.