Reliability:

Cybersecurity is a process where you must anticipate attacks and adapt, the organization must ensure that it must spread through its operations. Cybersecurity faces array of evolving and sophisticated attacks, organization must adapt to ensure its safety to these new threats.

Approach to cybersecurity requires an assessment of the potential risks if an attack happens. Organization should know what could happen if an attack successfully hits a component or system, and develop mitigations.

Factors of Safety:

* Keep software up-to-date
* It is important to keep software up-to-date because these updates contain security patches, adding security features, enhances existing features, fix bug issues, and improves performance for the devices.
* Use Antivirus and Antimalware software on the electronic devices
* Antivirus and Antimalware software prevents malicious programs from harming your computer. It also prevents malware from entering your computer.
* Use strong passwords
* This prevents hackers from succeeding in guessing your passwords.
* Backup your data
* By having a backup of your data, you can recover it in case that your data is lost or breached.
* Use two-factor authentication
* You will be alerted if someone attempts to access your account, and you can block them from accessing it.
* Always read the terms and conditions of any site
* You need to know if the sites will collect your information or not.

References:

* Kelley, K. (2023, October 25). *What is Cybersecurity and Why It is Important?* Simplilearn.com. https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security
* Khan, A., & Khan, A. (2023, October 12). *Cyber safety - definition, rules, and importance*. Intellipaat Blog. https://intellipaat.com/blog/what-is-cyber-safety/
* https://library.e.abb.com/public/fca5bce187ad45c585c0e5f383417c3b/4CAE001393-Balance\_Reliability-Cybersecurity-white-paper-A4-Rev1.2.pdf?x-sign=82NHGGVzwrVu2gyNykerRBQ1DQreB0XbjoHlfD2zcmzk3Mdel6lHB8siNwZjlKUm