**Importance of Information Security**

Information security is critical in today's life because as new technologies are being developed, cybercriminals are coming up with new ways every time that they can use to access organizations' systems. Therefore, information security has various importance in businesses, organizations, and companies, these include; firstly, information security helps reduce data breach risks and attacks that target the IT systems. Second, information security is responsible for data encryption, making sure that even when there are breaches in IT systems, the data accessed makes no sense to the attackers since they cannot decrypt it, also; to avoid IT system attacks, information security helps develop and chose which firewalls will best suit the IT systems, keeping them safe. Finally, information security preventing data breaches and IT systems attacks helps organizations and individuals relieve them of the losses they would have to face in data breaches, primarily by having too heavy fees resulting from legal actions and recovery plan costs that involve data breach investigation.

When it comes down to unauthorized access of organizations’ or companies’ information, information technology comes up with security controls and how to apply them to prevent individuals who are not authorized from getting their hands on information that is supposed to be private. The security controls that information security comes up with include measures that can be taken to prevent physical information theft or destruction. Information can be stolen or destroyed through fire breakouts or physical damage to devices storing the information (Ahmadi & Shybt, 2020). In addition, information security comes up with solutions like cloud storage where an authorized individual can access all the information they need even after losing it from their primary storage.

Some individuals and organizations use very brief and weak passwords to protect their devices and data. Information security helps in such cases by helping them develop strong passwords that can protect their devices and data for a lifetime. additionally, information security exposes individuals to risk assessment tools that help them identify vulnerabilities that may be present in their systems and which can do a lot of damage if not patched.

**Components of Information Security**

There are three significant components of information security which are availability, integrity, and confidentiality. First, the significant component is confidentiality; this component is connected to secrecy most of the time, aligning with encryption. In information security, confidentiality means that data is available only to individuals that are authorized. If data can be accessed by parties that are not authorized, its confidentiality levels are deficient.

The second component is availability, which means that information is readily available when required by an authorized person. Information security insists that for a system to prove its availability it channels of communication, computing systems, and security controls must be functioning correctly.

The other component is integrity. This component sees no tampering with data from when it is uploaded for transmission to when it is being stored in the database (Legárd, 2020). There would be no data integrity if the data were intentionally or not subjected to any form of unauthorized modification.

**Information Systems Protection**

There are several ways of protecting information systems, and some of them include the following; protecting them with strong passwords. Many attacks that have succeeded in the past are due to users using weak passwords. Therefore, coming up with strong passwords is a good way of protecting information systems. Another way to protect information systems is by designing safe systems whereby you minimize or limit those people who access the technology infrastructure you use; this minimizes failure points securing information systems. Additionally, most attacks on information systems happen due to individuals being careless or uninformed; therefore, providing them with basic training will help reduce mistakes associated with information systems, thus keeping them safe. Finally, ensuring that sensitive data is not stored in the cloud can help reduce attacks on information systems. Unfortunately, these third parties safeguarding your information can also have security issues that leave your sensitive information exposed to more threats.