# E potfolio

There is absolutely no doubt in stating that electronic systems are more efficient than manual ones in today's time. They are not only faster, moreaccurate and cost efficient, but also perform the magical task of analyzing and grouping data from different information systems and databases from different locations. For companies who expand into many sub branches or go multi-national, online information systems act as the backbone of the management, making them easy to handle. However, while working with online databases, some ethics must be kept in mind. Technology today makes it very easy to gather, store, communicate and likewise, manipulate data. Consequently, developments in information systems also involve social and political relationships-and thus ethical consideration in how information is used is all the more important. Government records, workplaces and private lives of the people are within the reach of the system and it is a vital responsibility now to balance the needs and rights of everyone. While everything with online security systems seems very user friendly and tends to make life easier for a management team, there is also a significantly dangerous side to the use of online information systems. One of them happens to be cyber crime. Typically, cyber crime can be divided into four categories; theft, fraud, copyright infringement and attacks. With the popularization of the internet and its several weak links, hackers find it possible to break into security systems where they have access to a person's key personal data such as social security numbers, date of birth, driver's license numbers and credit card information. Affected individuals have experienced fraudulent financial transactions, and false accusations of crimes they have never committed which begin showing against their names on their personal record files.

Information systems are vulnerable to physical attacks, electronic hacking, viruses and natural disasters. With computer systems serving as the backbone of many organizations, managers must be aware of the both: the risks and the opportunities to minimize the risks to information systems. A virus is a computer program designed to infect another computer without its permission or knowledge of the user. It can spread from one computer to another, by either sending it over a network, for instance, the internet, or by carrying it on removable media such as CDs, DVDs, USB drives etc. A virus has the tendency to destroy an information system, deleting the data and making it forever irrecoverable. To look on the bright side, these threats to the information systems can be fought with some security measures. The main goal is to protect the confidentiality, integrity and availability of information. The system security is generally limited to guaranteeing the right to access a system's data and resources by setting up authentication and control mechanisms that ensure that the users have rights that are only granted to them. To ensure that there is no vulnerability of an information system being attacked, the following must be kept in mind: Identify the security needs and the IT risks of the company. Outline the rules and procedures that must be implemented. Monitor and detect the information system's vulnerability and keep updated about the system's flaws Define the actions to be taken in case a threat is detected. However, security must also go beyond employee knowledge and cover the following areas as well: A physical and logical security mechanism that requires employees to continuously supervise the information system. A procedure for managing updates. A properly planned back-up strategy. An up-to-date documented system. An active firewall to fight malware. Even though an information system is prone to much attack, it can be overcome by taking into account such measures and while there is no denying of the fact that a computer information system is the vital key to the success of an expanding company, it is justifiable to say that such consideration be given to its information system. Reference Lodrick, Karen. " Identity theft and cybercrime statistics in picture graphs." San Francisco, CA. March 29, 2010. Web. June 1, 2011.