

## **Abstract**

The increased deployment and use of communications technologies in recent decades has resulted in a consequent increase in risk, as each technology brings with it a set of associated vulnerabilities.

The use of information technology (IT) in business is on the increase, as more organisations are becoming dependant on IT infrastructure as they move away from the traditional manufacturing industry to a more knowledge based industry.

The use of IT by these companies allows them to gain a competitive advantage over companies that have not made the transition to the digital economy. IT also allows organisation's customers to reap the benefits, as new business media are available to them, i.e. Retailing (Point Of Sale, POS), online banking, emailing private information etc.

Although a heavier reliance on technology offers organisations convenience, they must be aware of the hidden dangers that technology can bring, especially as more and more organisations are going online each day. We may not realise it, but some knowledge of Internet Security is important when surfing the web. This thesis, therefore, documents key incidents of exploitation involving security breaches online, showing how they not only affect the companies involved but how the general public can become embroiled in such incidents without prior knowledge. This thesis also documents the vulnerabilities that were exploited in each incident and the countermeasures that may be used to stop or detect such attacks from happening in the future. The motives of the attackers are also examined in order to establish why such attacks are becoming a daily occurrence in this digital age. Then finally the actions of organisations are examined to see why companies allow themselves to become easy targets for such attacks by deploying systems that they know have a reputation for being vulnerable to attack.