**P3 – Explain the potential risks to an organisation of committing to an e-commerce system.**

**Introduction**

In this report, I will explain the potential risks to an organisation of them using an e-commerce system.

**Hacking**

Hacking is someone who seeks to weakness and gains access to a computer system, or a computer network. Hackers are always doing these unexpected results to gain access to the data. The ways that these attacks could happen is by finding out the identified target, potential ways of these attacks and exploiting the system. To protect the data, you can use secure the system by banning unnecessary and unsafe websites that the user explores, scan the system for any viruses, and they are many other ways to secure the system. The effects it has on the e-commerce websites is that they could break into the website by purchasing, or abusing, any customer information that is not right. They could get information from another person’s account, and they could be purchasing products that the user does not even know about.

**Firewalls**

The benefits of using firewall are that it secures the computer network. It disallows other networks from entering your secured network. As it blocks other networks, it blocks viruses and hackers from entering the network. It acts like a secure “wall”. It does not let anything past it. For organisations that have secure data on their computers, it is vital that they tell/ask all employees to keep their firewalls ON. It is important and if anything is let past, it can access the files and the virus can spread/multiple quickly. The disadvantages of using firewall are that it acts like a central point of attack for intruders; and if they are passed firewall, they have access to the whole network. In addition, it only protects one point of it, it does not protect the other parts of it e.g. modem. The effect of using firewall on e-commerce is that it blocks any unauthorised users gaining access to any information that is not allowed by the user. The effect on an e-commerce website is that it can gain access to all of your information if the firewall has been broken in too. This needs to be looked after too, as well as the computer.

**Viruses**

The technology has increased drastically and they are number of issues that the business needs to become aware. Malware is one of the risks that the business needs to solve. Malware is a malicious software that disturbs the network to gain access to private information of any network. Malware is not just a one virus, but it includes a number of issues such as worms, Trojan horses and spyware. To prevent his from happening, of course, each computer needs to have an anti-virus to get rid of these malicious attacks. Malware could be on what the user uses to on websites i.e. the user visits a website full of malware. Once they click on the ‘fake’ advert, the malware can gain access to the account. To resolve this situation, the IT administrator in the business can prevent and block the website from gaining access to the virus account. In addition, having an anti-virus, it could show the user that the website is safe or unsafe.

**Identity theft**

This is when someone uses someone else’s identity to gain access to their personal belongings, or purchase any product in their name. Some types of personal belongings they could use is the following: name, credit card, number, committing crime, and many other. This is used within a website, because some people could get some products from the e-commerce website, without seeing their face, and the original person not knowing about it. This could be a hectic ride for the business, because if the original user finds out that these purchases have been made, he could want a return. This results badly for the business.



**Conclusion**

As discussed, these are just some of the potential threats that Tick Tock need to consider. Some of these threats can be reduced by installing software and remaining vigilant. These threats could be faced whenever, and when alerted, it should be removed immediately. Scanning an anti-virus software could remove the viruses, but not all. Some of the users need to be aware of what sites they browse. This is, because some sites are not safe for the user, nor computer, to use.

**Reference**

* <http://en.wikipedia.org/wiki/Identity_theft>
* <http://en.wikipedia.org/wiki/Firewall_(computing)>
* <http://en.wikipedia.org/wiki/Hacker_(computer_security)>