Business ethics paper on cyber-liability assignment

Art & Culture

The third party also carries his or her own share of the liability. Vicarious liability can arise in situations where one arty is supposed to be responsible for (and have control over) a third party, and is negligent in carrying out that responsibility and exercising that control. For example, an employer can be held liable for the unlawful actions of an employee, such as harassment or discrimination in the workplace.

Even though the employer is not the one who committed the unlawful act, the employer is held liable because it is considered responsible for its employees' actions while they are on the job and it is considered to be able to prevent and/or limit any harmful acts performed by its employees. The employer may e able to avoid vicarious liability by exercising reasonable care to prevent the unlawful behavior. Another common source of vicarious liability occurs when a child behaves negligently.

The parent can sometimes be held vicariously liable for the child's actions. One situation where this might occur is if a child injures or kills someone while driving. Vicarious liability was also define as the tort doctrine that imposes responsibility upon one person for the failure Of another, with whom the person has a special relationship (such as parent and child, employer and employee, or owner of vehicle and driver), to exercise such care as a reasonably prudent person would use under similar circumstances.

To claim under the tort of vicarious liability, firstly, someone should know all the requirement of vicarious liability should be establish first in order to claim under the tort of vicarious liability. The requirements are as the following:- There must be a wrongful tortuous act There must be special

relationship between employee-employer The tort must occur within the course of employment Example Of Case Of Vicarious Liability:- (I) Leister v Helsel Hall Limited (2001) This case is about the sexual abuse by a warden of a school boarding house o a student.

The issue of this case is whether the warden's action in abusing the pupil was closely connected with employment would it be fair and just to hold his employers liable. Result: The company which owned and ran the school was responsible for the warden conduct as the warden responsibilities include the welfare and safety. It was considered that vicarious liability would not apply to other employees. (ii) Limps v London Omnibus and Co. In this case, the driver of the bus in order to overtake another bus was driving in a very rash and negligent manner and hence ended up injuring the plaintiff.

The catch in this case is such a tendency was known to the employer and he had prohibited the driver from doing so. Result: Clearly the servant has acted negligently and the master then becomes vicariously liable. (iii) Rickets v Thomas Tilling Ltd. The driver who had been authorized to drive the bus, feels tired and asks the conductor to drive the bus for some time. The conductor while driving the bus, does so quite negligently and hurts a pedestrian X.

X brings a suit against the bus company. Will he succeed? Result: By a clear application of the principle Of wrongful delegation, it is quite conclusive that the master is liable. Hence X will succeed. (2) Cyber-Liability Any organization operating a Web site or conducting e-business needs protection from an invading army Of exposures, such as e-theft, destruction of critical

data, defamation, libel, copyright or trademark infringement, e- vandalism, e-threats, denial of service, and more.

Cyber-liability is focused on the ever-increasing risks and rapidly evolving liability exposures associated with the creation, transmission, security and storage Of data, particularly private, personal and proprietary information. Today’s businesses face the threat of hackers trying to steal data, and the accidental disclosure of such information, or loss of such information can give rise to liabilities to customers, clients and the government. Cyber-liability addresses the first and third party risks associated with e-business, Internet, networks and informational assets.

Cyber-liability insurance coverage offers cutting edge protection for exposures arising out of Internet communications. The concept of cyber liability takes into account first and third party risks. The risk category includes privacy issues, the infringement of intellectual property, virus transmission, or any other serious trouble that may be passed from first to hired parties via the Web. Cyber-liability is composed Of two defined risks:- (I) Security Liability Security liability is the unauthorized access / use of a utility (or vendor/ partner/ independent contractor) network.

In 2007, the exposure increasingly involves the theft of mobile computer equipment such as a desktop server or a laptop to perpetrate data theft. It is well known that many cases involve inside employees who have trusted access into the network. Employees or trusted third parties with access into the network can steal identity information, critical business information,

transmit malicious code, and articulate in a denial Of service attack against network or the network Of others.

This risk includes paper documents, as well as electronic data. (ii) Privacy Liability Privacy liability is the violation of privacy laws or regulations that permit individuals to control the collection, access, transmission, use, and accuracy of their personally identifiable medical and / or financial information. The most serious civil and regulatory exposure surrounds personally identifiable non-public information; however there are risks associated with disclosure or theft Of confidential corporate data Of others.

Cyber liability insurance protects against compensation claims arising from:- Staff misuse of company email (for which you are responsible), or the content on your website or blob, that defames or libels a third party System damage caused by viruses or mallard you may have transmitted (u knowingly) via email or the internet Security breaches that give unauthorized access to confidential data Financial losses caused by the failure of a company website, the collapse of your internet provider or the work of computer hackers Why all organizations and peoples should consider and have it (cyber liability insurance):- Provides visualized protection Often not included in general liability policies protects your financial interests against the greater risks associated with a high profile online presence, even if a claim against you is invalid Minimizes the disruption to your business of managing your way back to normality in the event of any incident Question 2: List the top categories of litigation of cyber-liability.

In general, sanctions could include “ exclusion from entitlement to public benefits or aid; temporary or permanent disqualification from the practice of commercial activities; placing under judicial supervision; judicial winding-up; ND also temporary or permanent closure Of establishments which have been used for committing the offence”. Sanctions imposed would have to be “ effective, proportionate and dissuasive” in order to be justified. One of the top categories of litigation of cyber-liability is hacker attack. Hacker means someone who tries to break into computer system and enjoys doing the computer programming rather than just theorizing about it.

Hacker will be a proficient programmer or engineer with sufficient technical knowledge to understand the weak point in security system in the computer. This hacker attacks can take legal action if the person is arrested for involving highly private files in the case of national security. There is some case in February 1 999, where Ministry Of Defense Satellite has been hacked by a small group Of hackers gained control of a MOD (Ministry of Defense) Keynes military satellite. They manage to reprogram the control system before being discovered. Therefore, no arrests have been made by U. S Air Force. Breach of privacy also can be defined as a hacker attack. A breach of privacy occurs when there is unauthorized access to any personal information. According to Daniel J. S (2008), privacy is apparent in today’s society as individuals hold more and more “ personal” information spread to the public. Based on this statement, sites owners or the business owners should keep the users’ personal information in confidential and also should not get reach by the other users’. In online shopping website, the owner should private their customer’s information such as their personal details

such as name, address and contact numbers in the website. When it viewed by other consumers that have violence the rights of the consumers, it may cause litigation. Cyber fraud is also one of the top categories of litigation of cyber-liability.

Cyber fraud refers to any type of deliberate fraud for invalid or illegal profit that OCCUrs in online. Fraud occurs when trickery was used to gain a dishonest advantage which is often financial over to another person. There are four types of fraud which is individual fraud, corporate fraud, online fraud and advance free fraud. The most common form is online credit card theft. Paid product purchased through online auctions and no delivery Of merchandise or software is common form of monetary cyber fraud. The example of fraud ease is on March 2007 at Koala Lump where Noradrenalin was sentenced by court to serve 50 months jail after pleading guilty to fraudulently withdrawing ARM 1. 4 million from a Tabbing Hajji account. She also sentenced to 24 months for a second transaction that she had made using forged identity card in the name of other people identity. Question 3: Draft a nine on cyber-liability for students in University Malaysia Saba. There are some guidelines that can be used by MUMS students regarding cyber-liability. These include:- (I) E-mail Students must always remember that they are communicating with other human being. They must introduce themselves, be courteous and tolerant. E- mail also can become public, so never write anything that would make them concern. Always be careful when choosing a subject heading.

The most important thing is that they must ensure they give a clear idea of what the e- mail is all about. Avoid writing in capital letters for more than a word because it can be as shouting. (ii) Social Networking Site Don’t post personal information, such as telephone number and address carelessly. Must always be careful with all information that they post. Don’t give any password to anyone. Before post the photos or anything, think first. Arsenal photos should not have revealed any information that can give negative impacts. Just add people as friends to the site if they know that particular person. Always check the privacy setting of the social networking site. This is to make sure that there are no people trying to steal their information. Iii) Computer Virus Every student must have installed anti-virus software to protect their information from being stealing and also to protect their gadget. Don’t ever open any suspicious e-mail. Don’t download anything from sites that are not legal or from other unapproved sites. (iv) Boards / Blob Inappropriate comments must be unacceptable. All comment will be published on discussion boards, so students need to be aware before gives any comment. Consequences of breach of these protocols may need requirement of a retraction, disciplinary action and removal of any comment deemed to be inappropriate. So, students need to be careful.