|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Full Harvard Style Reference | Title of Ethical Disaster | Short Description of what happened.  (250 words max) | Could this have been prevented? If so how?  (250 words max) | How does this disaster relate to the BCS Code of Conduct? |
| Bcs.org. (2017). Code of conduct | Membership | BCS - The Chartered Institute for IT. [online] Available at: http://www.bcs.org/category/6030 [Accessed 15 Dec. 2017].  Forester, T. and Morrison, P. (2001). Computer ethics. Cambridge, Mass. [u.a.]: MIT Press, pp.105-115. | USS Vincennes  guns down Iranian civilian airliner | On the 3rd of July 1988, an American naval ship is patrolling the outskirts of the Persian Gulf. Its defence system which was called the Aegis was the fault for this incident. It was tested and the system was meant to be able to track hundreds of targets in a 300 kilometre radius and fire at 20 targets at a time. Whist patrolling, the system spots what it thinks is a fighter jet and proceeds to warn the aircraft. There was no response, so warship starts to fire at the plane and the civilian air craft is destroyed. There were no survivors and 290 lives were lost. | Before the Aegis system was even put on to the American warships, it was tested and came with poor results. When tested it was displayed 3 targets and a total of seventeen to shoot down. The system managed to miss six of the targets down to software errors. Furthermore, the system was tested in a cornfield in New Jersey and had no testing in the environments where it would have to work in. Even if proper testing was carried out in the right environment, the system should have been checked after the appalling target test. The whole disaster could have been prevented if the right testing had gone into the system and the fact that it had never occurred shows a lack of care. | This disaster relates to the BCS code of conduct in two ways. The first being that the error cost 290 civilian lives. In the code under “Professional Competence and Integrity f) avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction.” This disaster breaks the code as no action was taken on the failed testing attempts and people were killed because of it. |
| Bcs.org. (2017). Code of conduct | Membership | BCS - The Chartered Institute for IT. [online] Available at: http://www.bcs.org/category/6030 [Accessed 15 Dec. 2017].  Forester, T. and Morrison, P. (2001). Computer ethics. Cambridge, Mass. [u.a.]: MIT Press, pp.105-115. | Ney York Bank crash | On the 20th of November 1985 The Bank of New York was trying to process around 32,000 bank transactions. There was a system error and the problem was that the bank was sending out money to people at the wrong times as the system had crashed. The bank had to borrow money from the federal reserve as it was over drawn by 32 billion. The system was fixed the next morning but had the cost the bank 5 million in interest for the loans. | The banks software crash was down to the system handling the ingoing and outgoing transactions corrupted. The computer systems started to corrupt and change the transactions themselves. Therefore, the bank didn’t know what to pay and was in danger. This disaster couldn’t have been prevented because the systems crash wasn’t down to human error just the systems malfunction on humans. On the other hand testing should have been conducted to check if the system could handle a max amount of transactions. | The disaster relates to the code in “Public Interest a) have due regard for public health, privacy, security and wellbeing of others and the environment.” This is because the systems lost the company 5 million and that would have been representing as ordinary people that work at the bank would have lost a lot of money maybe putting their wellbeing at risk. |
| Bcs.org. (2017). Code of conduct | Membership | BCS - The Chartered Institute for IT. [online] Available at: http://www.bcs.org/category/6030 [Accessed 15 Dec. 2017].  Forester, T. and Morrison, P. (2001). Computer ethics. Cambridge, Mass. [u.a.]: MIT Press, pp.105-115. | London’s ambulance dispatch system malfunction | In October 1992 a new dispatch system was introduced to the ambulance system in London. Again the system had a poor testing history and after going live the system was overloaded and started malfunctioning. The system directed several ambulances to the same place and some people were never seen to. This was a massive error and endangered the public. | The system that they created has a bad history, being used in the North East. There was many problems when introduced there and the fact that London is a largely more populated city, the problems would only get worse. This could have been prevented because there was never a backup system put in place which would have at least worked if the main system crashed. If there was it would have at least worked better than the new system. Furthermore, if the people who create the system improved it after the appalling attempt in the North East it would have been fixed. | The disaster relates to the code under “Public Interest a) have due regard for public health, privacy, security and wellbeing of others and the environment.” This is because the system put people living around London in danger as they might have not been seen to by the ambulance and therefore could have died. Also under “Professional Competence and Integrity f) avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction.” This is because if they were to put in a backup system like any system of this magnitude would need, they could have prevented the error affecting the public as much as it did. |
| Armerding, T. (2017). The 16 biggest data breaches of the 21st century. [online] CSO Online. Available at: https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html [Accessed 15 Dec. 2017].  Ft.com. (2015). Cyber security: Attack of the health hackers. [online] Available at: https://www.ft.com/content/f3cbda3e-a027-11e5-8613-08e211ea5317 [Accessed 15 Dec. 2017]. | Anthems Hack | Anthem, a health insurer based in America had a hack. This exposed and used the details like names, where people lives and their social security numbers placing them into the hands of the hackers. This would allow the hacker to very easily perform identity theft on any of the people’s information that was stolen. The breach cost the company 100 million dollars. 78.8 million people were affected as the network server was breached. | The hack of the system had took a very long time but was extremely easy and down to complete idiocy. One of the workers that was using a computer connected to the system had opened a phishing email which then proceeded to infect the system by installing malware and viruses to the computer. This could have been prevented if people that worked at the company were giving the right IT training and could Identify these types of scam emails. | The disaster relates to the code under “Public Interest a) have due regard for public health, privacy, security and wellbeing of others and the environment.” This is because the system endangered the customer’s identities and wellbeing as the hackers could easy conduct identify fraud on anyone’s details that were stolen. |
| Armerding, T. (2017). The 16 biggest data breaches of the 21st century. [online] CSO Online. Available at: https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html [Accessed 15 Dec. 2017].  En.wikipedia.org. (2017). SHA-1. [online] Available at: https://en.wikipedia.org/wiki/SHA-1 [Accessed 15 Dec. 2017]. | Adult Friend Finder hack | Adult Friend Finder, an adult hook-up website which people would use to meet others was breached in October 2016. The hackers were able to get 20 years’ worth of data in no time at all. The types of things that were stolen was names, passwords and addresses which could be used to identify people using the website. | The system that was hacked had one glaring, easily breach able point and that was the actual passwords. The passwords were protected an algorithm which would change the password into a 160 bit hash value and stored. The SHA-1 hashing algorithm was extremely poor and didn’t stand a chance against the hack. If a better system was used to protect the passwords of users then this hack most probably wouldn’t have happened. | This disaster relates to the code under “Public Interest a) have due regard for public health, privacy, security and wellbeing of others and the environment.” This is because the privacy of the users was broken and identities were revealed. It also relates to the code under “Professional Competence and Integrity c) develop your professional knowledge, skills and competence on a continuing basis, maintaining awareness of technological developments, procedures, and standards that are relevant to your field.” This is because the system that was used to protect the data was outdated and not useful at all. The hacker could penetrate this system easily. If the people that put this in place would have realised this the hack might have not happened. |