

Ethical Issues

by Me You

Submission date: 15-Jul-2019 03:20PM (UTC-0500)

Submission ID: 1152144007

File name: Ethical_Issues_and_Information_Technology.doc (42.5K)

Word count: 1550

Character count: 8032

Ethical Issues and Information Technology

Student's Name

Institutional Affiliation

Ethical Issues Regarding Information Technology

In the current society, there have been numerous security breaches of technological systems. Despite the fact that there is modernization, invention and innovation in the information technology industry, the number of attacks in the industry is equally alarming. These attacks involve attacks of telephones, rampant malwares in soft wares and thus, businesses have been experiencing a series of problems (Smith & Wong, 2016). An overview of possible security breaches is thus important. Some of the common security breaches in information technology include installation of malicious software, hackers altering the operating system, physical interferences with computers, employees interfering with the information technology system and the password being compromised. An example of a major information technology breach recorded in the information technology industry is the Yahoo breach in the years 2013 to 2014.

Description of the Company Affected

In the year 2016, Yahoo came out to speak of a major security breach that it had experienced in the year 2013 and 2014. While in the middle of negotiations for the company to sell itself to Verizon, the company experienced a major security breach which left an impact on approximately 3 billion users doing away with their business with the company. The company suspects that the security breach was performed by a state-sponsored actor (Smith & Wong, 2016). In this attack, email addresses of Yahoo users were compromised. In addition to that, the attack compromised the telephone numbers and names of Yahoo users. The robust bcrypt algorithm was used to perform the attack and the technology helped in hashing the passwords of Yahoo clients. Prior to this attack, there had been a similar hacking in 2013 though it was conducted by a different group of people. And in addition to the passwords, date of birth, email

addresses and names that were interfered in 2014, in this attack security questions and answers were tampered with.

I selected this case specifically because of its impact on the clients. Clients utterly value their privacy and protection of their information from breaches. In this attack, more than 3 billion clients shifted from yahoo to other service providers. This is an adverse negative impact on a company and it was catastrophic considering the company was selling itself. As a result, the company had to negotiate with Verizon and in the process of negotiation; Yahoo lost \$350 million due to the security breaches (Vayena, Salathé, Madoff & Brownstein, 2015). In the business world, a single dollar is precious. And thus, with such a huge loss, I selected the case to serve as a perfect example of the impacts of security breaches in information technology.

Implications of the Breach In Terms Of Privacy Laws and Violations of the Law

As a result of this breaches, there were a number of changes that were made in the privacy laws. There were changes in the criminal conduct. From an analysis of the Yahoo attack, it is evident that the government hired an attacker into the private company. It is suspected that the Russian government was responsible for hiring the proxies to attack the company. Some of the reasons for this hack were to extort money from the company, and to steal data from the company as well as ruin the company's image (Smith & Wong, 2016). And thus as a result, privacy laws were enhanced such that user credentials were and are to be a hacker gold. In this case, when user credentials are treated as gold, it provides authorized access to the online account user. It will thus be difficult for a hacker to access a user's information.

Impact of Technological Breaches on Consumer Safety and Well Being

One major impact of technological breaches is the loss of customer trust. As experienced in the Yahoo breach, there was a rampant rise in the degree of customer mistrust. Specifically,

clients who had a direct impact by their emails being attacked and their information hacked developed a lot of mistrust in the company (Smith & Wong, 2016). As a result, they quit from business with the company and opted for alternative service providers where they felt their data and information is safe.

Technological breaches also increase the degree of cautiousness in customers and it raises customer awareness. Customers are also willing to pay a high amount of money provided their data and information is kept safe and secure. Thus, when making purchase decisions and choices on the type of website provider they want to use, they will always consider the security risk involved in the company. For a company like yahoo, given its past history, most consumers will shy away from the company and opt for its competitors (Miller & Blackler, 2017). Besides, breaches play a role in educating consumers about their right to privacy of information. It is through a breach of information technology that consumers learned they have a privacy right to their information in websites. Some customers sued the company because the contents of the leaked information were crucial and quite personal. Though suing of the criminals may be difficult and may take long, the breach raised awareness that the customer does not have exclusive rights to your information and data. Your data and information is personal despite the fact that they own the website.

Leakage of some private information shared through emails may be fatal and it may lead to dangerous situations. Through information systems like emails, people schedule meetings, share their financial transactions and even some personal information like medical history. For example, a doctor can share the results of an X-ray scan to the president through his or her email. When the competitors of the president during the presidential election gain access to such vital information, they may use it to campaign against their competitor (Laudon & Laudon, 2015).

And in such a scenario war may arise between the supporters of the competing presidential candidates. Thus, security breaches may lead to wars when crucial and personal information is leaked to the public. Thus, it puts the life of the client at risk.

Recommendations to Improve and Protect Privacy of Its Clients

There are a number of recommendations that I would suggest for the company. The company can invest in proactive and reactive security measures. While proactive measures prevent the occurrence of a security breach, reactive measures involve reducing the impact of an attack (Floridi & Taddeo, 2016). With modernization in information technology, there are new measures that can be used in both proactive and reactive measures. Some proactive measures involve the use of encryption whereby data can only be accessed after decryption. In such a case, only few people have an access to the security codes for decryption such that in the case of a hack, the company can identify who was responsible for the breach.

A reactive measure in the case of an attack can be through honesty and notification. In this case, the company should empower clients with an easy access and notification model. This is whereby; the clients can notify the company of the breach as well as the clients can notify one another in the occurrence of a breach. In such a scenario, the company will provide a mitigation process whereby the number of affected clients shall be decreased (Miller & Blackler, 2017). In addition to that, the company can notify its users about the breach and request them to help prevent further loss and attack on their information by following some clearly stated procedures. Long waiting processes and delayed responses from website service providers in Yahoo Company may have been a major cause of the huge losses experienced by the company.

Another major security proactive measure is investing in an intrusion detection system. This system shall enable early detection of an unauthorized user who is trying to log into the

system or an intruder who has just logged into a system (Floridi & Taddeo, 2016). Though the purchase of the intrusion detective system will be expensive, it is cheaper as compared to the losses experienced in the occurrence of an attack.

Lastly, I would recommend for harsh treatment of the hackers. This is by giving them an imprisonment that is equivalent to the degree of harm they have caused to both the online users and the company. And since the hackers were hired by the state, the company should thus request for a government-requested sentence (Laudon & Laudon, 2015). For this sentence, the government encourages victims of hacking attacks to report suspected hackers. And since every hacker desires for a government sponsored sentence, it should encourage people to report hackers. With adequate cooperation of victims, the company, the court system and the government, the degree of attacks on information technology will decrease.

Reference

Floridi, L., & Taddeo, M. (2016). What is data ethics?.

Laudon, K. C., & Laudon, J. P. (2015). Management Information Systems: Managing the Digital Firm Plus MyMISLab with Pearson eText--Access Card Package. Prentice Hall Press.

Miller, S., & Blackler, J. (2017). Ethical issues in policing. Routledge.

Smith, L. C., & Wong, M. A. (Eds.). (2016). Reference and Information Services: An Introduction: An Introduction. ABC-CLIO.

Vayena, E., Salathé, M., Madoff, L. C., & Brownstein, J. S. (2015). Ethical challenges of big data in public health.

Ethical Issues

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7
