Computer Crimes

Name

Institution

Date

**Introduction**

 Even as businesses continue to embrace and depend on computer technology and electronic data transfer to run their daily operations, there is a significant growth in the amount of data that is passed from one point to the other and stored online yet the security of this data is not guaranteed. This has left the security of data highly compromised and the exposure of this data raises the levels of liability an organization can bear in cases of a data security breach occurs. This is confirmed by the high interest in ensuring cyber and cyber risk and the increasing awareness of the range of risks one is likely to face in dealing with online data transfer and storage.

**Discussion**

There are various types of cyber-crimes. They include; hacking, Cyberstalking, online identity theft, online child abuse, ransomware attack, and internet fraud (Gordon & Ford, 2006). Hacking involves unauthorized access to a device is it a smartphone or a computer. Cyberstalking uses the internet and other forms of online platforms to interfere with peoples’ privacy, harass them, con or blackmail them into some pressure. In extreme cases, Cyberstalking can lead to abduction, rape, physical attack, and murder. Online identity theft is the act of a person stealing someone else’s personal information. This has been achieved through phishing emails, injection of malware and hacking by brute force. It is one of the most serious cybercrimes, especially where a financial institution or an account is taken over and money is withdrawn or transferred. Ransomware attacks take the form of injecting malware into organizations’ devices in order to gain access to data and demanding some payment by holding the organization to ransom. Finally, internet fraud also referred to as online scams involve an unsuspecting party willingly giving money to buy a nonexistent item or service. These payments are usually hefty sums of money and the victim realizes when the paid service or good cannot be delivered.

 Of the three million cases of identity theft reported last year in the United States, a quarter involved loss of money. This was an increase of $ 406 from $375 in 2017. A case in hand is that of King in an identity theft case scheme in 2013 where he came online purporting to own a record label by the name Dower Music Entertainment which would offer jobs to a number of people. This was seen as an opportunity to several people who applied and were invited for interviews in Manhattan and King identified himself as the CEO, hired the applicants as interns to work from home to work as interns on unpaid terms with a promise of permanent terms. Through this, he was able to get the identity of employees and he went ahead to apply for a credit card in his name and obtained a loan of $29,000 using another employee’s name. Further, he bought a car and jointly registered it under his name and that of another employee later for ti to be involved in an accident from which he claimed $8886 without including the registered employee (Roberts, Indermaur & Spiranovic, 2013). In another scheme, he ran a company named Upstate Family Transport and hired a driver whom he later used his details to purchase a Mercedes Benz worth $58000. He claimed to be the driver to the van and drove it away. All these crimes happened through a stolen identity that had been posted online.

 The other case of cybercrime is hacking and this one is common to banks. A case in hand is the hacking is the cyber-attacks that happened between 2015 and 2016 via the SWIFT banking network where millions of dollars were stolen. These attacks were carried out by the APT group of hackers. Their strategy was exploiting vulnerable systems of the banks and the hackers would take control of the bank accounts. They would in turn request for transfer of funds from the bank and these requests appeared legitimate. Through this, the hackers would in turn gain money from the unsuspecting banks (Trautman & Ormerod, 2016). The central bank of Bangladesh was the first to detect the threat and this was followed by an attack reported by Vietnam. In both cases, malware was used to write authorization messages while hiding that such messages had been sent. It is these messages that would steal the cash, then messages would be deleted to make sure no revelations of transfer of funds and finally, any confirmation messages would be blocked. Where the reports would be printed, the malware would alter the report before it got to the printer. Similar cases also were reported in Ecuador where the money would be transferred to Hong Kong China.

 Data breaches have happened in the recent past in many places. Companies that experienced these attacks compromised records, damaged the company’s reputation and breached peoples’ privacy. In 2013 across 2014, Yahoo experienced an attack that affected about three billion account holders. As it was preparing to sell itself to another company, Verizon, it reported that it had suffered a big data breach and suspected state involvement. The results of the attack were a compromise of the names of account holders, email address compromises and change of personal phone numbers and dates of birth. An algorithm was used to bypass passwords. After the incidence, they realized that the breach had affected more users and this time security questions had been altered. As a result, yahoo lost a whopping $350 on the sale price eventually getting $4.48 billion with an agreement to share the liability of the breach with Verizon (Page, Kaur & Waters, 2017). It is after the sale that they changed the name from yahoo to Altaba, Inc. the value of the company dropped from $100 billion to $93 billion.

 The effects of cyber-crime are not only felt society online but also offline. The effects, especially of identity theft, can bring a total change of one’s life including loss of property and business. Costs of security as well come in and this reduces the profit of the organization in question (Trautman & Ormerod, 2016). Finally, piracy has been the biggest undoing in the music and software industries where players lose millions of dollars every year to pirates. The impacts are quantified mainly based on the amount of revenue lost or losses incurred like is in the case of Yahoo and Swift banks.

**References**

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13-20.

Page, J., Kaur, M., & Waters, E. (2017). Directors’ liability survey: Cyber attacks and data loss—a growing concern. Journal of Data Protection & Privacy, 1(2), 173-182.

Roberts, L. D., Indermaur, D., & Spiranovic, C. (2013). Fear of cyber-identity theft and related fraudulent activity. Psychiatry, Psychology and Law, 20(3), 315-328.

Trautman, L. J., & Ormerod, P. C. (2016). Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach. Am. UL Rev., 66, 1231.