Sony: the world's largest data breach

Technology, Information Technology

Sony: The World’s largest Data Breach? The internet has become vulnerable due to presence of many hackers ready to pounce on anycontrol and security breach in systems, to make a fortune. Though the internet is a strange world that has not been perfectly maneuvered, firms have tried to incorporate different security systems though sophisticated hackers still get access to such systems. However, in some cases, lack of proper security mechanism and controls are to blame for such hacking of sites. The Sony security breach on its online video game network may be considered as one of the cases, where companies fail to maintain the required security against such hacking threats, breaching client’s security as happened in one of the largest security breaches involving Sony Corp. 1. One of the possible security weaknesses and control measures as Sony affirmed was negligence in security details when developing the software that supports and runs such a network. According to Laudon and Laudon (229) the use of fixed internet devices that have permanent connections to internet eases identification by hackers. Therefore, though Sony Company understood this, they could have compromised security of the software as they hurriedly moved to design new products to ensure market leadership. Such blunders could have exposed codes with errors making it vulnerable to hackers. Moreover hackers could have accessed the network through an administrator’s PC, who possesses the rights to access sensitive and classified information regarding Sony and its customers. Hackers were also suspected to have created false alerts using credit card through about three credit card bureaus in the U. S, which the company recommended for further investigation. The company also could be in a case where current or previous workers could have been

involved in the security breach as they understood the company’s system and codes; they were better placed to have configured the entire system resulting in such a massive security breach. Sony had numerous exploitable weaknesses which made the attackers to have an easy access to such a large number of accounts. The company lacked in intrusion and firewall system measures, which offer in depth security against such threats. 2. As Verizon (2) explains, where data leaves the organization, the company has no oversight over the data making it hard to control data threats. Therefore, people could have been involved in that there were business relationships with third parties with whom data was shared. Man error could have led such data to be lost or was deliberately manipulated through a fraudulent activity. Technology could have resulted in installation errors, programming errors, or an individual making unauthorized changes, which compromised such security (Laudon and Laudon 229). The fact that such games are permanently hooked to the internet as explained means hackers would have an easier time targeting them. The organization in its haste to develop new technologies as fast as possible, or improve the existing ones as well as in mass production was ignorant in ensuring quality control through strict auditing of all security system to avoid such security breaches. The security breach could also have been from one of the employees with access to such classified information who negligently used an open mail with no security encryption, or deliberately comprised the security of the system by leaving their stations unattended and open, where a third party could have taken the opportunity to leak valuable information for a considerable benefit. Since the breach was conducted by an external threat in the name of “ anonymous”

(Rashid, 1), this confirmed the proposition that the internet is extensively wide, and extensive advancement in hackers implies no security measure is perfect enough to prevent such breaches; though the company has to ensure the necessary maximum security conditions are met. 3. The security breach had costly implications to Sony as a company and to its customers at large. The fact that more than 101 million user accounts were stolen implies that personal information of all the users were accessed (Rashid, 1). Baker and Finkle (2011) explain though it is not clear how the hackers would use the information of customers. There were genuine concerns that such information may lead to vulnerability of the customers to further losses in credit cards, and unfair use of the information in impersonation. Moreover, most under age children had registered with their parent’s names; this information puts such people at grate risks though it might not be clear how they would use such information. On the other hand, the company suffered heavy losses due to this security breach. Sony generated more than $500 million in annual revenues from this service (Baker and Finkle, 2011). This implies that the hackers could have raked in considerable amount of cash from the company as the breach had gone unreported for number of days (about three days). However, the company was not concerned with the money lost, but with compromised information to their customers. Moreover, the service users were switched off and could not play for about seven days, which was unfair and a negative corporate image to Sony. The company also damaged its corporate image for not reporting the breach to authorities, and to its customers for several days, which was criticized. Hackers could have used such confidential information to the determination of the users. 4. One

way that such system security could be insured against any hacking is advanced encryption standards (Baker and Finkle, 2011). The company may implement data encryption that exceeds the available market standards to ensure their systems are secured. The company has also to tighten its internal security measures by ensuring those responsible for handling confidential information of such customers observe the highest ethics possible, and ensuring to be persons of credible standing with enough security mechanism implement in the working stations to prevent any third party for accessing. As the company acknowledged, there could have been errors in installing system, its design or negligence of workers making the codes available to hackers. Though the company has to rush in producing more technologically advanced products, there has to be quality controls to ensure that already produced services and products meet the highest standards of security and have been properly coded and encrypted. Laudon and Laudon (232) observe that some networks such as WI- Fi networks may be intercepted easily by use of sniffer programs that obtain the addresses to access resources of a certain network without authorization. The company has to take appropriate measures to ensure such spying programs do not penetrate their systems. All data breaches are initiated with an event later resulting to data loss. Entities causing such incidences are known as threat agents. Actions of such hackers are in most cases malicious, intentional and are carried out for a variety of motives. The fact that the internet is too wide, and the sophistication hackers have makes it difficult to prevent such security breaches, with more and more companies falling prey to such threats. In order to insure against such threats, there is need for utmost care

and diligence in software and system developments and installations, as well as observing the highest level of security standards to protect the company and customers to cases similar to Sony security breach, where millions of accounts were hacked making millions of people vulnerable as their confidential information was obtained. Work Cited Baker B. Liana and Finkle Jim. Sony PlayStation Suffers Massive Data breach, The Reuters, 26th April. 2011. http://www. reuters. com/article/2011/04/26/us-sony-stoldendata idUSTRE73P6WB20110426 Accessed 8th Dec. 2012. Laudon, Kenneth and Laudon Jane. Essential of Management Information Systems 10 Edition Book, London: Prentice Hall, 2012 Rashid, F., IT Security & Network Security News & Reviews: 10 Biggest data breaches of 2011 so far May 25, 2011 http://www. eweek. com/c/a/Security/10- Biggest-Data-Breaches-of-2011-So Far-175567/ Accessed 8th Dec. 2012. Verizon. 2012 Data breach Investigations Report Data Breach Investigations Report. 2012 Retrieved from http://www. verizonbusiness. com/resources/reports/rp_data-breachinvestigations report-2012_en_xg. pdf. Accessed 8th Dec. 2012.