Heartland Payment System Data Breach

Student Name	**Jasmeet Singh Narula**
Student Number	19210675
Programme	Ms in Computing (MCM1)
Module	CA640 – Professional and Research practice
Date of submission	15 November 2019
Word Count	2345 Words

An essay submitted to Dublin City University, School of Computing for module CA640 Professional and Research Practice, 2018/2019. I understand that the University regards breaches of academic integrity and plagiarism as grave and serious. I have read and understood the DCU Academic Integrity and Plagiarism Policy. I accept the penalties that may be imposed should I engage in practice or practices that breach this policy. I have identified and included the source of all facts, ideas, opinions, viewpoints of others in the assignment references. Direct quotations, paraphrasing, discussion of ideas from books, journal articles, internet sources, module text, or any other source whatsoever are acknowledged and the sources cited are identified in the assignment references. I declare that this material, which I now submit for assessment, is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work. By signing this form or by submitting this material online I confirm that this assignment, or any part of it, has not been previously submitted by me or any other person for assessment on this or any other course of study. By signing this form or by submitting material for assessment online I confirm that I have read and understood DCU Academic Integrity and Plagiarism Policy (available at: http://www.dcu.ie/registry/examinations/index.shtml)

Name: Jasmeet Singh Narula

Date: 15th November 2019.

Introduction

Personal data and security related attacks have always been a limelight of a rich resource, a resource which major corporations around the world hold and try to safeguard. Even with all the possible methods and protocols in place, some or the other individual or a group of individuals tend to find a loophole in the security feature to gain access to unauthorised sensitive data. Such sensitive data was targeted during the breach of Heartland Payment System in 2008 where the infiltrators made off with data of around 130 million credit cards and debit cards.

Literature Review

With over 80 billion transactions in a year and an average of 11 million transactions in a day, heartland payment system provides payment solutions to approx. 275000 businesses making it the 6th largest payment processor in US. [1] Company founded in 1997 had it headquarter in Princeton NJ. With a company, being one of the Fortune 1000 and handling millions of transactions a day, bound to have really sensitive data. This data in the hand of a felonious individual or group could be disastrous. The same happened in Jan 2009 where the company went public with an official statement of having a data breach. The breach came into the picture when payments giants Visa and Mastercard alerted Heartland of certain suspicious activities they observed with the transactions being done.

Heartland's then president and CFO, Robert H.B. Baldwin, said in his public statement "We found evidence of an intrusion last week and immediately notified federal law enforcement officials as well as the card brands, We understand that this incident may be the result of a widespread global cyber fraud operation, and we are cooperating closely with the United States Secret Service and Department of Justice." [2]

An immediate investigation was in place to 1. What data was compromised and 2. Find how the breach took place. On various investigations and audits a malicious software was found to be in heartland’s network system since 2008. It was observed that no Secure PIN, customer addresses and home phone numbers where compromised. What the hackers targeted where the credit and debit card details such as the number, expiry date. On further investigations by professional forensic and cyber security experts, a certain SQL injection along with ARP spoofing was smartly extracting customer data from different business systems. ARP spoofing is system of creating a spoofed message in the LAN to redirect the traffic through their system. The SQL Injection was used to gain access the Data base which stored the customer data through the payment processing systems.

In regards to the crime and cyber theft of data, Albert Gonzalez, a resident of NJ and a hacker, was arrested in August 2009 and was the main accused in the Heartland data breach. As the case proceeded, it was found that Albert was active between 2006-2008 and details of the breach came forward. Albert used SQL injections to infiltrate the security system of the company to extract the sensitive Credit and debit card number along with the additional card data to use it for commercial misuse and private monetary gain. As such attacks were not a single day’s work and required through background study, Albert had accomplices who assisted him in the whole operation. New details in the case revealed Vladimir Drinkman and Roman Kotov from Moscow, assisted Albert in the operation.

They were given the task to bring forward a list of companies by reviewing the list of all the fortune 500 companies. Once the to be targeted list was ready, they would then visit stores or branches to check out the point of sale payment system to get a better understanding. Along with visiting the physical stores, they would browse through the online websites to understand the vulnerabilities in their payment system.

Once the background work was complete, with the help of Mikhail Rytikov, who provided anonymous Web hosting services to the hackers to hide their activity, would lease computers hosted on different servers. They would then use the SQL strings to extract the details they required which were injected in November, 2007. Their aim was not only to hack the system once, but to embed a malware would give access to the data whenever they required. With this malware they would have the data of all the new customers as well. The malware was sophisticated that it readily evaded the antivirus software and the same was tested in top 20 softwares of that time.[2] Also, it had the feature to delete its trace by deleting the log files which were created. With the help of this malware the data was extracted multiple times between December 2007 and April 2008. Once this data was in-hand, it was then given to Dmitriy Smilianets, who then sold the stolen information and paid the attackers their cut.

For the crimes that he committed, Albert was sentenced for 20 years in prison. Even though Albert was arrested, the company had to face a series of troubles. They lost their PCI DSS compliance certificate due to the breach.[8] Approximately 130 million heartland payment system customer data were stolen due to which the losses and compensation we above $140 million.

Liffick Analysis Performed on the case

1. Ethical issues.

Albert along with other hackers created an environment where they unethically extracted computer software to gain unauthorised access to millions of data from the hosted company's servers. They not only stole the data to use it themselves but also once they got their cut, they distributed this data around the world for it to be misused without the consent of the owner of the data and his knowledge.

2. Main participants and actions

Primary Participants

i. Heartland Payment system management and customers.

Company that was hacked and had to face monitor losses as well as customers loyalty.

ii. Albert Gonzalez

He was the primary accused who carried out the hack, planned the process and brought the team together.

iii. Vladimir Drinkman

Vladimir assisted Albert in carry out the background study followed by hacking the system

iv. Roman Kotov

Roman assisted Albert in carry out the background study followed by hacking the system

v. Dmitriy Smilianets

Sold the data that was breached and paid the hackers.

Secondary Participants

i. United states of America's Government

The government and the district court of New Jersey were involved with the trial as along with Heartland, multiple such hacks had taken place. [3]

ii. Card Issue company

Companies such as Visa, Mastercard and American Express had to look into working together to fix the breach.

Implied Participants

i. Heartland Payment President, Technical Staff.
ii. Card companies' staff and management.

3. Reduced List

i. Heartland Payment system.

Heartland payment system was the company that was hit hard with the breach, had to face losses and had to work on bringing back to smooth functioning. They along with their customers were the primary victims

ii. Albert Gonzalez

He Masterminded the plan to hack the system, did the background work of visiting the stores, brought the team together, hacked the system.

4. Legal considerations

As part of the Legal case Proceeding, Title 18 of the united state code was issued on the case. Code 1030 was put in place to handle cases related to any fraudulent activity using a computer or servers.

- Title 18, United States Code, Section 1030(a)(2) – To use data and access the computer of an individual without their knowledge [3][4]

- Title 18, United States Code, Section 1030(a)(4) – Obtaining something of certain value from a computer. [3][4]
- Title 18, United States Code, Sections 1030 (a)(5)(A)(i) - transmitting a malicious code or program to cause damage. [3][4]
- Title 18, United States Code, Sections 1030 (a)(5)(B)(i) – Accessing a secure system without authorization. [3][4]
- Title 18, United States Code, Section 1349 – Selling /Re selling of unlawfully obtained resources. [3][4]

Apart from these legal Laws that were charged, many policies and laws of the companies would have been broken due to the unethical access to the system. Due to this breach, Heartland lost its compliance Standard code of PCI DSS which was required by companies for acquiring and keeping the customer card details safe.

5. Possible Options for participants

The Heartland Payment System Management could have:

- Invested in an inhouse cyber security team as the data that it holds is of a large value.
- Brought in new encryption techniques as a precautionary step
- Conduct regular audits to find any anomalies.
- Should bring the public to notice the breach to make the customers aware of the situation and give them a change to know whether they were affected of the breach.

Albert Gonzales could have:

- Used his knowledge to an advantage by diverting his attention from hacking and misuse to Ethical Hacking by assisting government and private organisations.

6. Possible Justification for Actions

The possible justification that the Heartland Payment system management would have had was:

- As this had never happened to the company before, assumption was that the system was optimised.
- Usually small alerts don’t mean a breach. Could have been a system error.
- The method of hacking using SQL injection along with a malware to extract and hide the task was new and wasn’t readily known which made the management unaware of an attack of this sort.
- As the Company was PCI DSS compliant, they were under the impression that no such attack could take place.

Possible Justification that Albert would have had:

- As he had readily been given a computer of his own at an age of 12[5], he had access to resources without guidance to use or misuse it.

- He was accused to be part of a young group of hackers called Shadowcrew which could have been the reason he was maybe lured into joining and using his knowledge for their profit. [6]

7. Key Statements

The following Phrases are important as part of the analysis.

- “At this point, though, we don't know the magnitude of what was grabbed."
- “Achieving PCI compliance does not imply that a business has achieved real security”
- “We understand that this incident may be the result of a global cyber fraud operation, and we are cooperating closely with the United States Secret Service and Department of Justice,"[11]
- “The warranty program will reimburse merchants for costs incurred from a data breach that involves the Heartland Secure credit card payment processing system” [11]

8. Questions Raised

Questions raised based on the Case are:

- As the business was handling critical customer data, was the data even secure?
- Is having PCI compliance enough to consider the data is or will be secure?
- Was there someone within the heartland payment system to have assisted the breach?
- Were the management even sure that the malicious code was taken care of and there wasn’t more piece of such codes present as they didn’t even know when it was sneaked in?
- Who should be the Judge to decide the correct actions have been taken?

9. Analogies and Related issues.

- Concurrently, Albert was also been accused of a similar data breach of an American department store, TJ MAXX in 2005 where more than 100 million customer card details were stolen and the breach was in place without a trace until 2007. Such attacks took place at the same time when multiple stores were being hit with the same period.
- Data from stores such as seven11 were also stolen by monitoring the POS in the store and the payment system was hit to gain access to the customer details.

10. Utilization of Code of Ethics within the case

Soo that the use of computing can be utilised for the benefit of the society and everyone around certain ethical codes were drafted. Such ethical and professional codes were misused in our case.[7]

- 1.2 Avoid harm.
- 1.3 Be honest and trustworthy
- 1.6 Respect privacy
- 1.7 Honor confidentiality
- 2.2 Maintain high standards of professional competence, conduct, and ethical practice.
- 2.3 Know and respect existing rules pertaining to professional work
- 2.8 Access computing and communication resources only when authorized or when compelled by the public good.

11. Alternative proposals within the case

Pessimistic Proposal

Albert was successful with planting the required code into the system back in 2007 and was highlighted in 2008. This led to increase in number of customers that were affected. As per the Annual reports, finances were hard hit as the breach caused drop in the market share.[9] A weak firewall which didn't stop or flag the breach along with delays in raising it publicly without being transparent was found to be disastrous for the company.

Optimistic Proposal

The code which was soon found and taken care of, was traced back to the primary accused. Company soon worked on bringing experts to restore the security architecture to avoid such breaches further. On the other hand, Albert with his knowledge and experience began helping the federal agency in finding cyber criminals. [10] Once his Plea Bargain is accepted, he could make a carrier as an expert in tracing cyber criminals while working with the government and other agencies.

Compromised Proposal

The case of Heartland Payment system was set as an example which brought a lot of security changes within the industry. New techniques being used by the hackers which were now put on spotlight due to which certain precautions were being taken by not just the affected company but thousands of others. New techniques such as End to End encryption, tokenization as well as Chip based technologies were invented to counter such disastrous losses due to breaches.

12. Conclusion

Heartland payment system's data breach was one of the biggest hacks which caused damages in terms of revenue, settlements along with human privacy which was an ethical violation. Coming out of such a setback takes its time but definitely bring something new to improve. The hack brought the technique to limelight which was then handled by a much more secure firewall. This breach proved just by having the compliance is not stopping the hackers and continuous assessment of the security structure is required to give client data the highest Priority in terms of safety.

13. Bibliography

1. Sherri Davidoff, Data Breaches: Crisis and Opportunity. Addison-Wesley Professional; 1 edition (October 26, 2019), Volume: 464 pages.
2. Kelley Jackson, Russian Hackers Sentenced in Heartland Payment Systems Breach Case. Available at https://www.darkreading.com/attacks-breaches/russian-hackers-sentenced-in-heartland-payment-systems-breach-case/d/d-id/1331080
3. Ellen Messmer, Network World (US). Heartland: 'Largest Data Breach Ever'. Available at https://www.csoonline.com/article/2123599/heartland---largest-data-breach-ever-.html

14. References

[1] Andrew Langford. 2016. Global Payments Completes Merger with Heartland Payment Systems. Available at https://investors.globalpaymentsinc.com/news-releases/news-release-details/global-payments-completes-merger-heartland-payment systems?releaseid=966563

[2] Jason Maloni. Jan 2009. Heartland Payment Systems Uncovers Malicious Software In Its Processing System. Available at https://web.archive.org/web/20090127041550/http://2008breach.com:80/Information20090120.asp

[3]USA V Albert Gonzalez Indictment. 2009. Available at https://web.archive.org/web/20090823200450/http://www.usdoj.gov/usao/nj/press/press/files/pdffiles/GonzIndictment.pdf

[4] Cornell Law School. U.S. Code § 1030.Fraud and related activity in connection with computers. Available at https://www.law.cornell.edu/uscode/text/18/1030

[5] James Verini, (2010-11-10). "The Great Cyberheist". The New York Times. Available at https://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html

[6] Sharon Gaudin. 2009. Government informant is called kingpin of largest U.S. data breaches. Available at https://www.computerworld.com/article/2527161/government-informant-is-called-kingpin-of-largest-u-s--data-breaches.html

[7] ACM Code of ethics. Available at http://www.acm.org/binaries/content/assets/membership/images2/fac-stu-poster-code.pdf

[8] Jaikumar Vijayan. Aug 20, 2008. Changes to PCI standard not expected to up ante on protecting payment card data. Available at https://www.computerworld.com/article/2532723/changes-to-pci-standard-not-expected-to-up-ante-on-protecting-payment-card.html

[9] Robert O Carr and Robert Baldwin Jr. 2009. Heartland Payment system Annual Report. Available at https://www.sec.gov/Archives/edgar/vprr/0901/09011991.pdf

[10] Eric Chabrow . April 2011. Gonzalez Seeks Guilty Plea Withdrawal. Available at http://www.bankinfosecurity.com/gonzalez-seeks-guilty-plea-withdrawal-a-3527

[11] Brain Krebs 2009. Payment Processor Breach May Be Largest Ever - The washington Post. Available at Phttp://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html