

Discount Mugs Data Breach

by Martin Albert

Submission date: 08-Mar-2019 05:51PM (UTC+0500)

Submission ID: 1089927318

File name: Discount_Mugs_Data_Breach.txt (5.24K)

Word count: 830

Character count: 4415

Title: Discount mugs data breach

Student name

Institutional Affiliation

OUTLINE

This paper seeks to discuss into details the events of data breaching incident experienced by Discountmugs.com in 2018. It will begin with introduction of the subject of cyber-attacks and data breaching. It will use the company as case study to relate to

the importance of compliance to PCI-DSS. In addition to this, the paper will also discuss industry standards its role and values to both the company and the industry.

INTRODUCTION

With the rise of technology and digital platforms, cyber security has risen to become part and parcel of our daily lives and worries. Thus to say, each and every user of the internet for transactions or personal use stand a chance of becoming a victim of a cyber-security attack. The major security incidents are usually known to arise from unsecured servers, cyber-attacks and phishing scams among others. When it comes to data breaches, the target in most cases is usually the commercial industry. This is the reason why the ¹Payment Card Industry- Data Security Standards (PCI DSS)

expect **all** organizations including **merchants and service providers** who by any chance store, transmit or process the data of card holders to comply with its set policies and show proof of compliance to their acquirer at least once in every year.

As a matter of fact, it has been reported that 96% of all victims of data breaches usually admit to noncompliance to the PCI-DSS. (Chuvakin, A., & Williams, B. R, 2012). This just proves that attackers usually target these organizations that have a weakness when it comes to compliance to the standards. That said, this paper will therefore focus on the online data breach experienced by Discountmugs.com in 2018 while discussing the incident into details.

DISCUSSION

Discountmugs.com is an online retailer that deals with custom giveaways. Between the months of August and November 2018, the company experienced a data breach where the attackers managed to place a malicious information-skimming code on the website's check out page. The malicious code placed at the checkout page of the website gave the hackers access to the information containing full customers payment card details such as phone numbers, email addresses, names, postal codes and even their physical location addresses. This attack was majorly aimed at siphoning off the customer's credit cards together with their personal information. The tentative number of people affected by this attack is estimated to be thousands following the number and amount of transactions that took place between the months that the data breach occurred. As a matter of fact, the website is ranked as one of the busiest in terms of web traffic considering the thousands of daily visitors.

Upon learning of the attack, the company took measures upon itself and launched an investigation whereby it contracted a leading computer security firm. It also ensured that to notify all the customers who were potentially affected by this attack and assured them of provision of identity theft protection services free of charge. In order to regain the trust of its customers, the company also assured them of their intention and will of taking further steps that will improve their security posture based on the findings of the investigation.

The most definite question that lingers in the mind is whether the company was compliant to PCI-DSS at the time of this attack. In order to answer this question, one should be able to identify the loopholes that led to this attack and if they were as a result of non-compliance to the PCI-DSS. In this case, Discountmugs.com was compliant to some of the requirements at the time of attack. This is because it surely has managed its data transfers securely, have strong encryption methods, has role based security and user authentication among other secure measures that comply with PCI DSS. However the attack occurred as a result of some of the IT security shortcomings that the attackers took advantage of to inject the malicious code. (Thomson, L. L, 2011).

Industry standards play a vital role in the economy of any country while contributing to its domestic as well as international and global competitiveness. Industry standards relieve companies of liabilities since companies are under the umbrella of the industry standards. However it should not relieve them from liabilities since companies have individual responsibility to comply with the industry standards. PCI standards do not share any responsibility in case of a breach. However I think that they should share

responsibility since they are the umbrella entity that provides the guidelines to prevent these breaches. Industry standards provide value in creating an environment for healthy competition and designing of new concepts, reduces research and development costs, reduces economic risks and impacts positively on company flexibility and supply chain management.

REFERENCES

Chuvakin, A., & Williams, B. R. (2012). PCI compliance [recurso electrónico]: Understand and implement effective PCI data security standard compliance. Sin Lugar: Syngress.

Thomson, L. L. (2011). Data breach and encryption handbook. Chicago: American Bar Association.

Discount Mugs Data Breach

ORIGINALITY REPORT

1 %

SIMILARITY INDEX

1 %

INTERNET SOURCES

0 %

PUBLICATIONS

0 %

STUDENT PAPERS

PRIMARY SOURCES

1

docplayer.net

Internet Source

1 %

Exclude quotes Off

Exclude bibliography On

Exclude matches Off