PCI Breach Trend Report

Data Breaches September 2015 – January 2016

Author: Mustafa El-Jarrah

SUMMARY

During the months September to January, Security Risk Management (SRM) ltd was contacted by a broad range of companies legally required to seek assistance in securing data breaches. The largest number of cases came from SMEs, usually online retailers.

Although it has been quite a while since the patch was released, the most common source of compromise was found to be through the Magento Shoplift vulnerability, which allows the intruder to insert an administrative level user to the database, thereby allowing them to insert malicious code to steal sensitive information and execute malicious actions.

Other attack vectors noted were vulnerable plugins installed on the major content management systems Magento or Wordpress. In the majority of the cases, the vulnerable plugin allows an external user to upload a malicious file such as a web shell and take control of the victim's website thereby allowing them to execute code and steal sensitive information.

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 their 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 to it may not only result in loss of customer trust but 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:

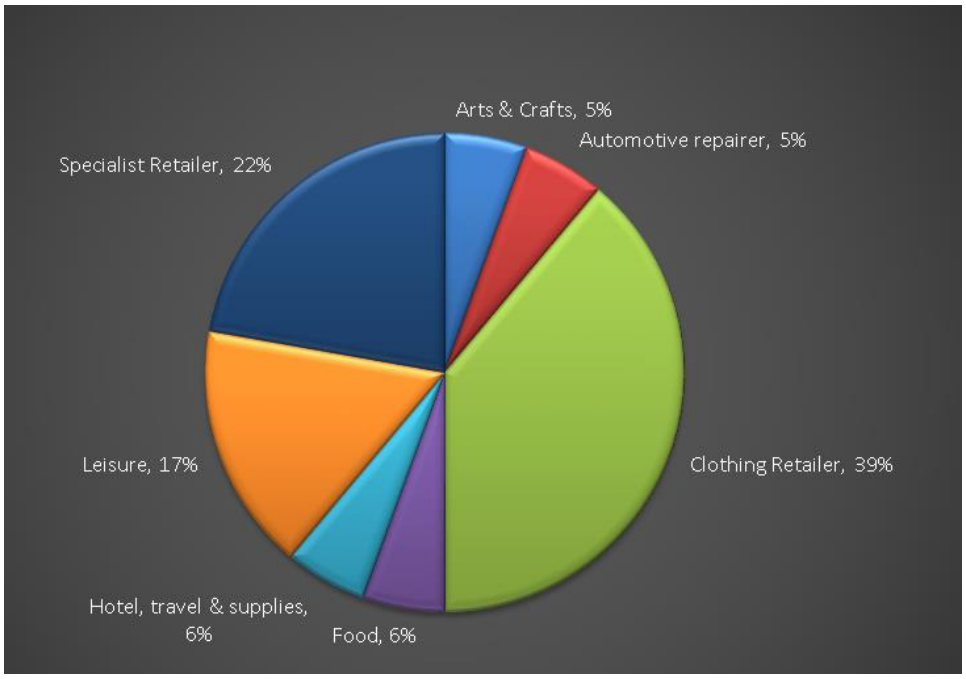
- A specific security management regime
- Protocols governing the design of software and its deployment
- Defined policies and procedures relating to the handling of card data, whether it be electronic or physical
- Regular technical verification checks, such as vulnerability scanning and technical testing

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 come 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.

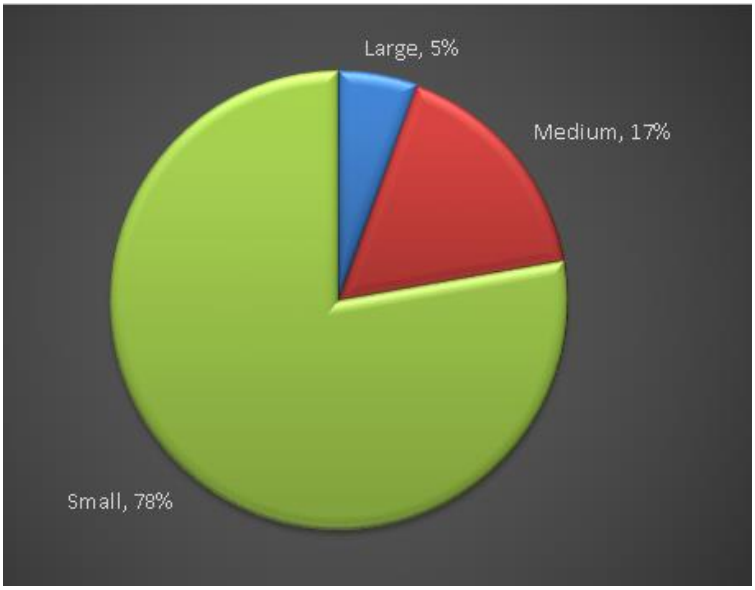
Ensuring you are compliant will significantly reduce your risk of a data breach, and will allow you and your customers to have peace of mind that data is secure. The responsibility for ensuring that card data is protected lies with the Merchant.

BUSINESSES TYPES AFFECTED September 2015 – January 2016

The pie chart below shows the types of businesses affected in the period September 2015 – January 2016.



The largest category was the clothing retailer (39%). In the majority of cases, these were small online businesses, selling niche products direct to the public.



Although SRM dealt with breaches across all size and types of businesses during the September 2015 – January 2016 period, the majority were SMEs as you can see from the pie chart above. 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.

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.

About

SRM is an Information Security specialist 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