

Breach Data Feedback towards Apt Security Measures

Inyene Udoh* Adewale Adebayo
School of Computing and Engineering Sciences, Babcock University, P.M.B. 21244 Ikeja, Lagos, Nigeria
*E-mail of the corresponding author: inyenepee@gmail.com

ABSTRACT
Information is very paramount in our day-to-day lives. Information systems need to be secure in fulfilment of their purposes. There have been failings in information security despite efforts to forestall them. Some needed feedback could be gotten through the analysis of breach data, which the research addressed. Data set of breaches on one of the leading repositories, Privacy Rights Clearinghouse, for the period between November, 1st 2012 and October, 31st 2013 was taken as a cluster and analysed. The analysis revealed that hacking was the most prevalent breach mechanism followed by stolen or lost portable devices and insiders perpetrated more breaches. Security efforts should focus more on perimeter and user device security and access control, especially in medical organizations. Insights gained from the timely analysis of breach data can help deduce apt security measures.
Keywords: breach data feedback, breach data analysis, security breach, breach countermeasure, security measures.

1.0 INTRODUCTION

We live in a society where we cannot do without information, which leads to a more developed society. This information is collected, manipulated or processed and stored by an information system. The information system needs to be secure. Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction (Wikipedia (a), 2013). Information Security is simply the process of keeping information secure: protecting its availability, integrity, and privacy.

Far more assets are computer-stored information such as customer lists, proprietary formulas, marketing and sales information, and financial data. Some financial assets only exist as bits stored in various computers. Many businesses are solely based on information – the data is the business (Demopoulos Associates, 2013). Effective Information Security incorporates security products, technologies, policies and procedures. No collection of products alone can solve every Information Security issue faced by an organization. More than just a set of technologies and reliance on proven industry practices is required, although both are important. Products, such as firewalls, intrusion detection systems, and vulnerability scanners alone are not sufficient to provide effective Information Security (Demopoulos Associates, 2013).

A data security breach can happen for a number of reasons. Some of which are loss or theft of data or equipment on which data is stored, Inappropriate access controls allowing unauthorised use, Equipment failure, Human error, Unforeseen circumstances such as a fire or flood, Hacking attack, and 'Blagging': offences where information is obtained by deceiving the organisation who holds it (Information Commissioner's Office, UK, 2012). Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, not to mention damage to the company's reputation. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement (Wikipedia (a), 2013).

A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property (Wikipedia (b), 2013). A number of industry guidelines and government compliance regulations mandate strict governance of sensitive or personal data to avoid data breaches (Rouse, 2010). Breach data is generated as a result of reports of data breaches. The breach data by its nature offers widely spread, unbiased, and easily accessible data for analysis to provide fresh insight into issues surrounding data breaches and information security (Shostack & Stewart, 2009). A couple of works have been done in analysing breach data, but it is necessary to examine current collection for fresh insights into what is happening presently towards apt security measures. Analysing the current collection of breach data to give fresh insight into data breaches as a result of security failures and lapses is very paramount.

The aim of this research is therefore to provide statistical analysis of breach data towards holistic data breach risk reduction. This will provide a perception into data breaches, a feedback, to help organizations implement more apt measures to secure their information or data.

Data set of breaches of one of the leading breach data repositories, www.privacyrights.org (Adebayo, 2012) for the period between November 1st, 2012 and October 31st, 2013 was taken as a cluster and analysed. The issues of data requirements, data generation method, sampling frame, sampling technique, sampling size, and data analysis, relating to gaining insight into breach data towards apt security measures, were addressed. The data obtained was analysed, using SPSS 21.0 for Windows Evaluation Version, along the following dimensions: number of records per incidence summary statistics, reported and percentage of reported storage breach incidents and storage records lost by organisation type, number of breaches and records lost by breach mechanism, number of breaches and records lost in time, number of records lost per incidence by organisation type, and number of records lost per incidence by breach mechanism, in order to communicate what could be learnt about storage breach events for improved informed breach risk reduction. No difficulty of being ethical was encountered.

There is a need to be aware of gaps or lapses in information security in order to be enlightened and be prepared to stem them. This research will provide necessary insight for better security of information in an organization and by extension, an improved and secure computing environment. The outcome of this research comes in the next section.

2.0 OUTCOME

Medical organisations (MED) suffered more breaches (42%) followed by BSR (15.1%), BSO and BSF respectively as seen in Table 1 and Figure 1. Hacking (HACK) is the number one breach mechanism (27.8%) followed by PORT (portable devices-19.0%), DISC (unintended disclosure) and INSD (insider) as seen in Table 2 and Figure 2. The breach incidents were mostly reported by the media followed by PHIprivacy.net and California Attorney General respectively as seen in Table 3 and Figure 3. Insider breaches resulted in the largest number of incidents (39.3%). There were 205 breach incidents from insiders in the various types of organisations as seen in Table 4 and Figure 4. Average number of records breached could not be ascertained (Table 5 and Figure 5).

3.0 LITERATURE REVIEW

Human errors and systems glitches caused nearly two-thirds of data breaches globally in 2012, while malicious or criminal attacks are the most costly everywhere at an average of $157 per compromised record (Ponemon Institute and Symantec, 2013). Ponemon surveyed nearly three hundred (300) companies across nine (9) countries. All of these companies had lost more than 1000 customer records and less than 100,000 (Ponemon, 2013). Total number of records containing sensitive personal information involved in security breaches in the United States is 608,087,870 in 3,763 data breaches since January 2005. (Privacy Rights Clearinghouse, 2013). According to DataLossDB, there have so far been five hundred (500) data breach incidents globally in 2013 and there were one thousand six hundred and twelve (1,612) incidents in 2012 (DataLossDB, 2013). In 2012, the Identity Theft Resource Centre (ITRC) documented 447 breaches in the United States, exposing 17,317,184 records. In the first half of 2013, there have so far been 255 incidents, exposing 6,207,297 records (Identity Theft Resource Centre, 2013).

As over the last couple of surveys, the two most expensive countries remain Germany and the US. It costs German companies an average of just under $200 for every record lost. In the US, that figure is $188. On the low end of the scale sit countries like Brazil ($58 per) and India ($42) (Symantec offers a Data Breach Calculator where you can guesstimate the cost of your organization's data losses.). One reason for the disparity is that the US and Germany are among the most heavily regulated when it comes to data breaches (Ryan, 2013). In the United States, data breach incidents cost companies $194 per compromised record. The average total cost per company that report a data breach in 2012 was down slightly at $5.4 million (Ponemon Institute and Symantec, 2013). The average cost per record of a healthcare data breach in 2011 was $240, which is 24 percent higher than average. Healthcare data breaches are the fourth highest by industry, behind the financial, pharmaceutical and communications sectors (Ponemon Institute and Symantec, 2012). Through 2016, the financial impact of cybercrime will grow 10 percent per year due to the continuing discovery of new vulnerabilities (Gartner, 2011). The average value of a lost laptop is $49,246 and the data breach costs represent 80 percent of the total cost of a lost laptop compared to two percent for replacing the computer. Encryption on average can reduce the cost of a lost laptop by more than $20,000 (Ponemon Institute and Intel Corp., December 2010).

In 2011, the average cost per record of a data breach in the financial sector was the third highest at $247, and 27 percent higher than average (Ponemon Institute and Symantec, 2012). Thus far in 2013, 3.5 percent of reported data breaches in the United States were in the financial services sector. In 2012, financial services data breaches

accounted for 3.8 percent of all reported data breaches and 470,048 total records (Identity Theft Resource Centre, 2013). Since 2005, 13 percent of data breaches globally recorded by the Privacy Rights Clearinghouse were in the financial sector, exposing 256,217,888 records (Privacy Rights Clearinghouse, 2013). In 2013, 48 percent of reported data breaches in the United States have been in the medical/healthcare industry. In 2012, there were 154 breaches in the medical and healthcare sector, accounting for 34.5 percent of all breaches in 2012, and 2,237,873 total records lost (Identity Theft Resource Centre, 2013). Since 2005, 25 percent of data breaches recorded by the Privacy Rights Clearinghouse were in the medical/healthcare sector, exposing 24,662,225 records (Privacy Rights Clearinghouse, 2013). Since 2002, 16 percent of data loss incidents globally involved the medical sector. Last year, 15 percent of data breaches recorded on DataLossDB involved the medical sector (DataLossDB, 2013). The education sector has one of the lowest costs of data breach at $142 per lost record, which is 27 percent lower than average (Ponemon Institute and Symantec, 2012). In the first half of 2013, 7.5 percent of reported data breaches in the United States were in the education sector and have exposed 168,145 records. In 2012, 13.6 percent of all reported data breaches were in the educational sector (2,304,663 records) (Identity Theft Resource Centre, 2013). Since 2005, 18 percent of data breaches recorded in the United States by the Privacy Rights Clearinghouse were in the education sector, exposing 10,695,778 records (Privacy Rights Clearinghouse, 2013). 14 percent of data loss incidents globally since 2002 involved the education sector. Last year, 12 percent of data breaches recorded on DataLossDB involved the education sector, less than any other industry sector (DataLossDB, 2013).

The majority of Intellectual Property (IP) theft is committed by current male employees averaging about 37 years of age who serve in positions including engineers or scientists, managers and programmers. About 65 percent of employees who commit insider IP theft had already accepted positions with a competing company or started their own company at the time of the theft. About 20 percent were recruited by an outsider who targeted the data. More than half steal data within a month of leaving. Three-fourths (75 percent) of insiders stole material they were authorized to access and trade secrets were stolen in 52 percent of cases. The majority of insider IP thieves (54 percent) used a network – email, a remote network access channel or network file transfer to remove or steal data. However, most insider IP theft was discovered by non-technical staff members (Shaw and Stock, 2011).

An insight into breach data showed that business organizations (36.8%) were the most attacked followed by medical organizations (27.8%). Hacking was top on the list of the breach mechanism (20.1%) and Insiders (26.8%) perpetrated more breach incidents than insider-malicious (Adebayo, Omotosho & Adekunle, 2012).

Business sector accounted for 60.6% of reported incidents, followed by government (17.9%), education (12.0%) and medical (9.5%). 76.8% of reported incidents were the result of external agents or activity outside the organization: hacking accounted for 68.2% of incidents and remained the number one breach type for the second consecutive year and 7.3% of reported incidents involved a third party. Insiders accounted for 19.5% of incidents (Open Security Foundation/Risk Based Security, 2013).

4.0 CONCLUSION

More serious attention should be paid to preventing hacking, to access control, and to user device security. Security practitioners are better informed about data breaches through proper capture and analysis of breach data (Adebayo, Adekunle & Omotosho, 2013). The continuous capture and analysis of breach data would help organizations that create, receive, store or transmit data avoid falling victim to a breach through the enlightenment it offers.

REFERENCES

Adebayo, A. O. (2012). *A Foundation for Breach Data Analysis*. Journal of Information Engineering and Applications, Vol. 2 No. 4, pp. 17-23

Adebayo, A. O., Adekunle, Y. A., & Omotosho, O.J. (2013). *System and Data capture framework insights into Breach data towards improved feedback*. Journal of Innovative Systems Design and Engineering, Vol.4 No.33, pp. 20-31

Adebayo, A. O., Omotosho, O. J. & Adekunle, Y. A. (2012). *Statistical Insight into Breach Data towards Improved Countermeasures.* Information and knowledge management, Vol. 2 No. 8, pp. 40-51

Demopoulos Associates. (2002). *What is information security?* Retrieved from http://demop.com/articles/information-security.html

Gartner. (2011). *Gartner Top Predictions for 2012: Control Slips Away*. Retrieved from http://www.indefenseofdata.com/data-breach-trends-stats/, November 30, 2013

Identity Theft Resource Centre. (2013). *ITRC Breach Report.* Retrieved from http://www.indefenseofdata.com/data-breach-trends-stats/

Information Commissioner's Office, UK. (2012). *Guidance on Data Security Breach Management*. Retrieved from http://ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/guidance_on_data_security_breach_management.pdf

Open Security Foundation's formerly Attrition.org (2013). *Data Loss DB*. Retrieved from http://www.indefenseofdata.com/data-breach-trends-stats/, November 30, 2013

Open Security Foundation/Risk Based Security (2013). *Data Breach Quickview: An Executive's Guide to Data Breach Trends in 2012.* Retrieved from http://www.riskbasedsecurity.com/reports/2012-DataBreachQuickView.pdf

Ponemon Institute and Intel Corp. (2010). *The Billion Dollar Lost Laptop Study*. Retrieved from http://www.indefenseofdata.com/data-breach-trends-stats/

Ponemon Institute and Symantec. (2012). *2011 Cost of a Data Breach: United States.* Retrieved from http://www.indefenseofdata.com/data-breach-trends-stats/, November 30, 2013

Ponemon Institute and Symantec. (2013). *2013 Cost of a Data Breach: Global Analysis*. Retrieved from http://www.indefenseofdata.com/data-breach-trends-stats/, November 30, 2013

Privacy Rights Clearinghouse. (2012). *A Chronology of Data Breaches*. Retrieved from http://www.indefenseofdata.com/data-breach-trends-stats/, November 30, 2013

Privacy Rights Clearinghouse. (2013). *A Chronology of Data Breaches*. Retrieved from http://www.indefenseofdata.com/data-breach-trends-stats/, November 30, 2013

Rouse, M. (2010). *Data Breach*. Retrieved from http://searchsecurity.techtarget.com/definition/data-breach, November 30, 2013

Ryan, D. (2013). *How much do data breaches really cost more you think?* Retrieved from http://www.itworld.com/it-management/361669/how-much-do-data-breaches-really-cost-more-you-think

Shaw, E and Stock, H. (2011). *Behavioural Risk Indicators of Malicious Insider IP Theft: Misreading the Writing on the Wall*. Retrieved from http://www.indefenseofdata.com/data-breach-trends-stats/

Wikipedia (a). (2013). *Information security*. Retrieved from http://en.wikipedia.org/wiki/Information_security

Wikipedia (b). (2013). *Data breach* .Retrieved from http://en.wikipedia.org/wiki/Data_breach

NOTE: The terms and abbreviations used to afford more clarity are as follows: Unintended disclosure (DISC) - Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email, fax or mail; Hacking or malware (HACK) - Electronic entry by an outside party, malware and spyware; Payment Card Fraud (CARD) - Fraud involving debit and credit cards that is not accomplished via hacking. Example is skimming devices at point-of-service terminals; Insider (INSD) - Someone with legitimate access intentionally breaches information - such as an employee or contractor; Physical loss (PHYS) - Lost, discarded or stolen non-electronic records, such as paper documents; Portable device (PORT) - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, and so on; Stationary device (STAT) - Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility; Unknown or other (UNKN); BSO - Businesses – Other; BSF - Businesses - Financial and Insurance Services; BSR - Businesses - Retail/Merchant; EDU - Educational Institutions; GOV - Government and Military; MED - Healthcare - Medical Providers; and NGO - Non-profit Organizations.

Table 1 shows the number and percentage of data breaches by Organization Entity.

Table 1: **Number and percentage of data breaches by Organisation Entity**

Organisation Entity		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	BSF	55	10.5	10.5	10.5
	BSO	72	13.8	13.8	24.3
	BSR	79	15.1	15.1	39.5
	EDU	44	8.4	8.4	47.9
	GOV	47	9.0	9.0	56.9
	MED	219	42.0	42.0	98.9
	NGO	6	1.1	1.1	100.0
	Total	522	100.0	100.0	

Figure 1 depicts number of reported breach incidents by organisation entity.

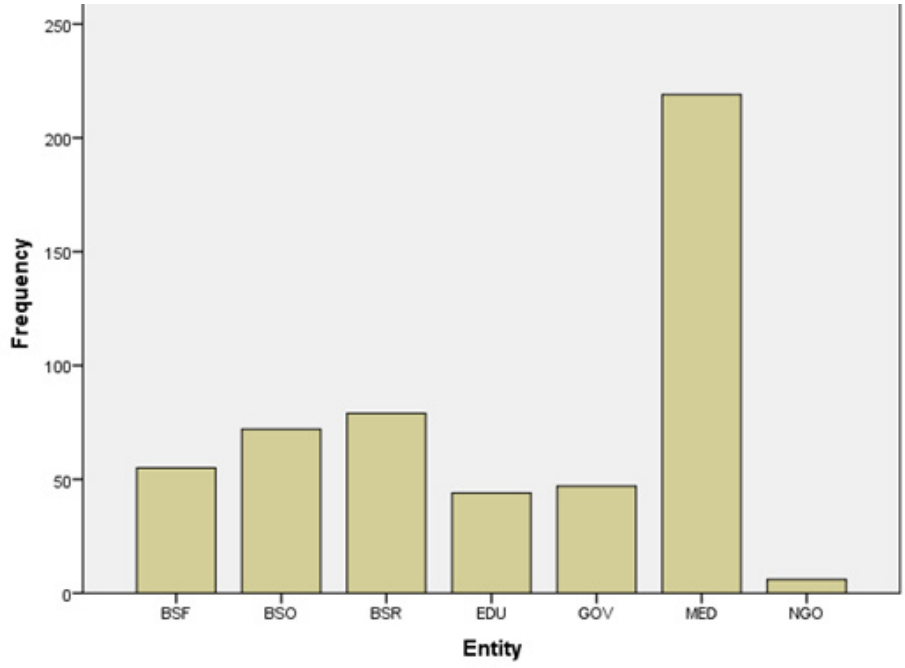

Figure 1: **Number of reported storage breach incidents by organisation entity**

Table 2 shows the number and percentage of breaches by detailed breach mechanism.

Table 2: Number and percentage of breaches by Detailed Breach Mechanism

Breach Mechanism		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	CARD	13	2.5	2.5	2.5
	DISC	96	18.4	18.4	20.9
	HACK	145	27.8	27.8	48.7
	INSD	87	16.7	16.7	65.3
	PHYS	49	9.4	9.4	74.7
	PORT	99	19.0	19.0	93.7
	STAT	19	3.6	3.6	97.3
	UNKN	14	2.7	2.7	100.0
	Total	522	100.0	100.0	

Figure 2 depicts number and percentage of breaches by breach mechanism

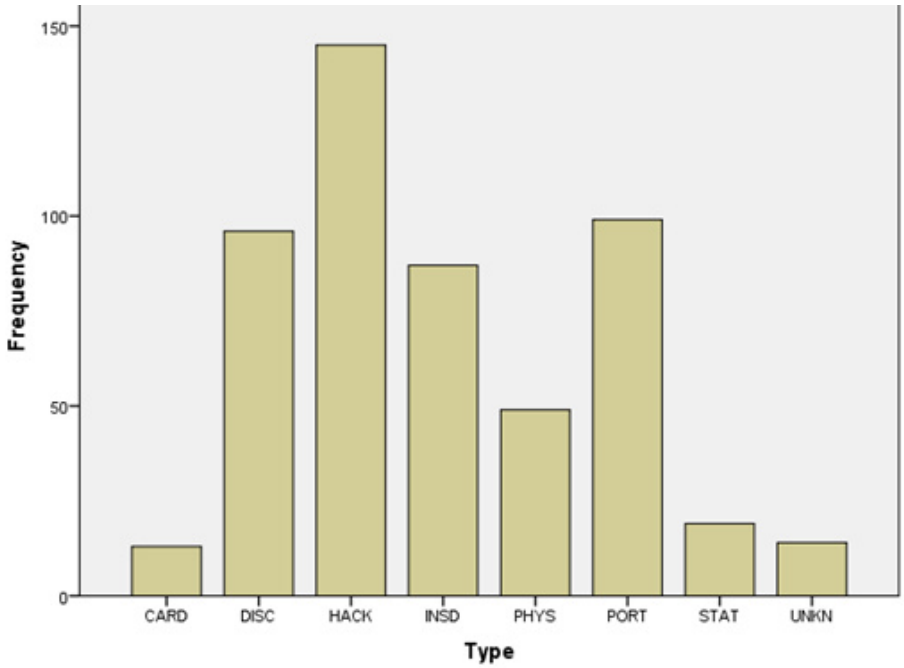

Figure 2 Number of breaches by Breach Mechanism

Table 3 shows the number and percentage of breach incidents by Information Source.

Table 3: **Number and percentage of breach incidents by Information Source**

Information Source		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	California Attorney General	99	19.0	19.0	19.0
	Databreaches.net	40	7.7	7.7	26.6
	DataLossDB	5	1.0	1.0	27.6
	HHS via PHIPrivacy.net	33	6.3	6.3	33.9
	Media	242	46.4	46.4	80.3
	PHIPrivacy.net	102	19.5	19.5	99.8
	Security Breach Letter	1	.2	.2	100.0
	Total	522	100.0	100.0	

Figure 3 depicts the number of breach incidents reported by information sources

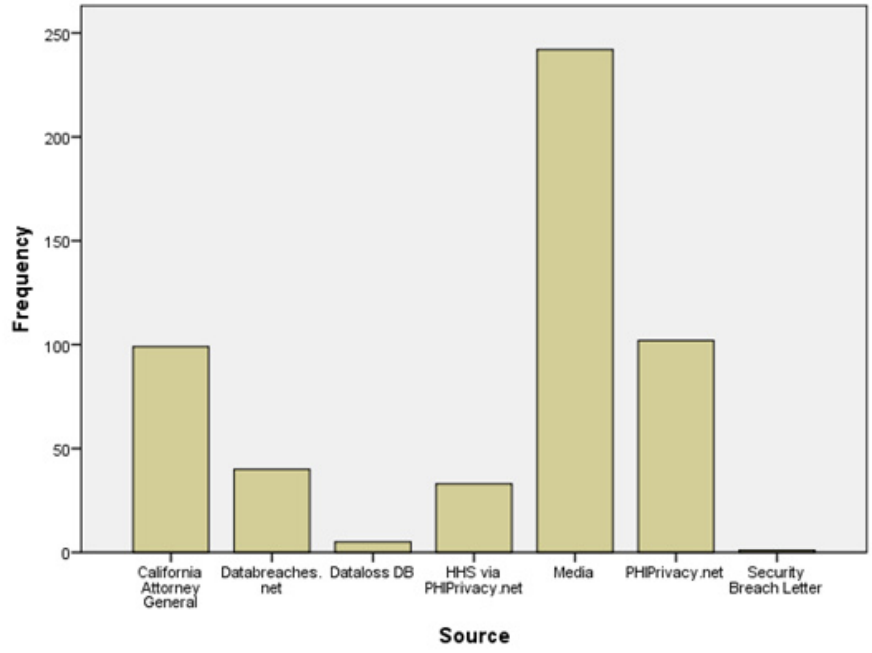

Figure 3 -Number of breach incidents reported by Information Sources

Table 4 shows number and percentage of breaches by Insider or Outsider.

Table 4: **Number and Percentage of Breaches by Insider or Outsider**

Insider/Outsider		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Insider	205	39.3	39.3	39.3
	Outsider	131	25.1	25.1	64.4
	Unknown	186	35.6	35.6	100.0
	Total	522	100.0	100.0	

Figure 4 depicts number of breach incidents by insider or outsider.

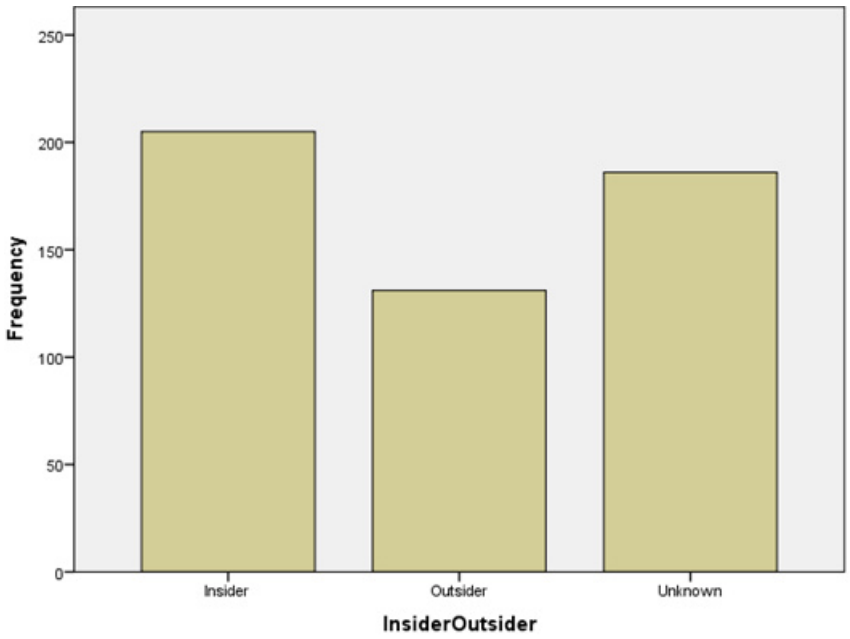

Figure 4 -Number of breach incidents by Insider or Outsider

Table 5 shows the number and percentage of records breached

Table 5: **Number and percentage of records breached**

Records breached		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Unknown	255	48.9	48.9	48.9
	< 1,000	79	15.1	15.1	64.0
	1,001 -100,000	166	31.8	31.8	95.8
	101,000 - 200,000	9	1.7	1.7	97.5
	201,000 - 300,000	4	.8	.8	98.3
	401,000 - 500,000	1	.2	.2	98.5
	701,000 - 800,000	1	.2	.2	98.7
	901,000 - 1 Million	2	.4	.4	99.0
	1Million and above	5	1.0	1.0	100.0
	Total	522	100.0	100.0	

Figure 5 depicts number of records breached.

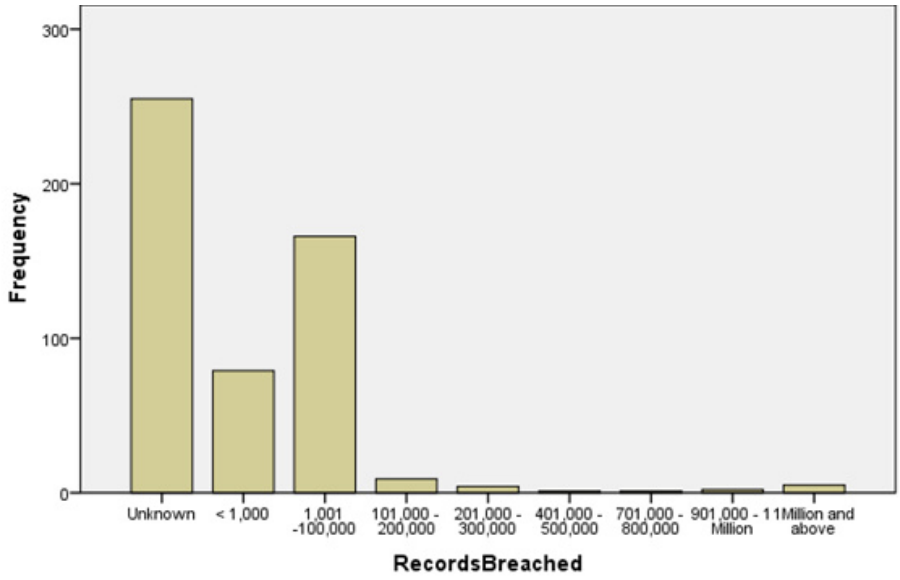

Figure 5 -Number of records breached