Global Data Breaches Responsible for the Disclosure of Personal Information: 2015 & 2016

J. Botha[1, 3], M.M. Grobler[2], M.M. Eloff[3]
[1]Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
[2]Data61, Commonwealth Scientific and Industrial Organisation, Melbourne, Australia
[3]Institute for Corporate Citizenship, University of South Africa (UNISA), Pretoria, South Africa

[1]jbotha1@csir.co.za
[2]marthie.grobler@data61.csiro.au
[3]eloffmm@unisa.ac.za

Abstract: Data breaches have gained extensive coverage as businesses and organisations of all sizes become more dependent on digital data, cloud computing and workforce mobility. Companies store sensitive or confidential data on local machines, enterprise databases and cloud servers. To breach a company's data one needs to gain access to restricted networks. Although this is a difficult task that requires specialised skills, hackers continuously identify vulnerabilities and loopholes to gain access and conduct data breaches. The Privacy Rights Clearinghouse[1] recorded 901,010,077 data breaches since 2005, with only 5,220 data breaches made public. In 2015 some of the world's largest recorded data breaches occurred; yet a total of only 266 data breaches were made public. 2016 still had a number of major data breaches and a total of 472 breaches were made public. When conducting business in the modern era, data protection and management of personal information have become an integral aspect for organisations and individuals. Despite increased focus on personal information and the existence of data protection legislation internationally, data breaches remain a common occurrence resulting in major cost implications. This paper investigates the most significant data breaches in 2015 and 2016 responsible for the leakage of personal information, with the aim of identifying a general trend in terms of data breaches and personal identifiable (PII) leakage.

Keywords: Data Breaches, Data Leakage, Hack, PII, Privacy

1 Introduction

An essential part of the digital economy today is security and privacy. Policies and legislations are being established world-wide to ensure that people around the world have an open and interconnected digital world (oecd.org 2013). However, even with comprehensive policies and privacy legislation already established in a number of countries across the world, data breaches are not only increasing in frequency, but also in breach size. It is possible to say that these breaches have now become a fact of digital life (Weise 2016). A data breach occur when personal identifiable information (PII) has been lost or maliciously stolen and therefore is at risk of being exposed (Romanosky, S. 2011). A data breach can result in large numbers of compromised records containing PII and could potentially lead to identity theft and other related crimes. PII can include an individual's government issued identification; contact information; birth date and place; online account information; medical, employment or financial records; biometric information and geographical information (FreedomidDirect n.d.). Attackers continuously discover methods and ways to intrude networks and steal private or confidential information. As such, cybercrime is rated as the number one national security threat by the USA Director of National Intelligence (Experian Inc 2016). At the time of writing, the Privacy Rights Clearinghouse (Privacy Rights Clearinghouse n.d.), reporting data breaches since 2005, recorded 906,388,226 breaches, with only 5,285 made public. The Identity Theft Resource Center (ITRC), also reporting data breaches since 2005, has recorded 5,810 reported breaches in total. Some of the largest data breaches ever were recorded in 2015, hitting the healthcare, financial, higher-education and federal markets. In some instances it even hit the security industry itself (Kuranda 2015). Research indicates that the medical and healthcare industry are increasingly being targeted by cybercriminals (Davis 2015).

This paper presents an overview, in Sections 2 and 3, of the most significant data breaches of 2015 and 2016, responsible for the disclosure of PII. The significance of a data breach is measured according to the type of data

[1] https://www.privacyrights.org/data-breaches

stolen as well as the number of records compromised and exposed, and not the cost or severity of the incident. Data is provided on the targeted company/agency; the country; the date of the data breach; the published date and the number of exposed records. Each data breach is categorised according to the sectors in which the targeted organisation operates. Other noteworthy security breaches that did not necessarily result in the exposure of PII are mentioned in Section 4. A comparative review on data breaches is provided, in Section 5, to identify whether the general trend in terms of targeted sector remains the same regardless of whether the data breach result in PII leakage. Data has been collected using existing literature, including governmental and private industry reports.

2 Most Significant Data Breaches of 2015

The number of data breaches in 2015 decreased marginally from the number of data breaches in 2014; however, the number of exposed records doubled from 2014 to 2015. In 2015, some of the world's largest data breaches occurred, but only 266 were made public (Privacy Rights Clearinghouse n.d.). The number of reported data breaches tracked by the ITRC in 2015 is 781, the second highest since 2005 (ITRC n.d.). Figure 1 indicates that 40% of the breaches originated from the business sector, nearly 36% from the health/medical sector, just over 9% from the banking/financial sector, about 8% from the government/military sector and over 7% from the education sector. The main motive for data breaches are financial gains. However, 2015 has seen a shift in motives towards obtaining personal information. The breached data is used to compel behaviour changes in breached individuals or groups, for social justice purposes and even to embarrass a nation (ITRC n.d.).

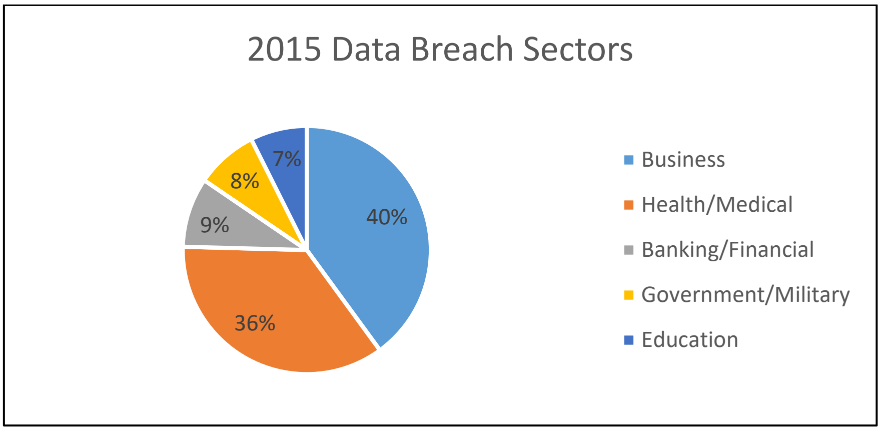

Figure 1. 2015 Data Breach Sectors (Compiled from ITRC n.d.)

Table 1 lists 23 of the most significant data breaches of 2015, sorted according to breached date. The following sections discuss the data breaches presented in Table 1 in more detail, grouped by sector. Where a breach is categorised in more than one sector, it will only be discussed once.

Table 1. Largest Data Breaches of 2015 (Compiled from IdentityForce 2015; BLI n.d.)

Company / Agency [Country]	Breached Date	Published Date	Records Breached (Approx.)	Sectors				
				Business	Health/Medical	Banking/Financial	Government/ Military	Education
Turkish Citizenship Database [Turkey]	2015.01.12	2016.04.04	49.6m+				✓	
Topface [Russia]	2015.01.20	2015.01.26	20m	✓				
Anthem [USA]	2015.01.27	2015.02.04	78.8m		✓			
JPMorgan Chase [USA]	2015.02.10	2015.11.##	100m+	✓				
TalkTalk [UK]	2015.02.27	2015.11.06	150k+	✓				
OOOwebhost/troyhunt.com [Global]	2015.03.30	2015.10.29	13.5m	✓				

Company / Agency [Country]	Breached Date	Published Date	Records Breached (Approx.)	Sectors				
				Business	Health/Medical	Banking/Financial	Government/ Military	Education
Office of Personnel Management (OPM) [USA]	2015.04.01	2015.06.##	22m				✓	
AdultFriendFinder.com [UK]	2015.05.21	2015.05.21	4m	✓				
Internal Revenue Service (IRS) [USA]	2015.05.26	2016.02.29	700k+			✓		
Gaana.com [Pakistan]	2015.05.28	2015.05.28	10m	✓				
Wattpad [USA]	2015.05.29	2015.08.07	40m	✓				
Bharat Sanchar Nigam Limited (BSNL) [India]	2015.07.04	2015.07.05	30m				✓	
Hacking Team [Italy]	2015.07.05	2015.07.29	1m				✓	
UCLA Health System [USA]	2015.07.17	2015.07.17	4.5m		✓			
Ashley Madison [Canada]	2015.07.20	2015.08.18	37m	✓				
Korea Pharmaceutical Info. Center [Korea]	2015.07.26	2015.07.26	43m		✓			
Experian/T-Mobile [USA]	2015.09.03	2015.10.01	15m	✓				
21st Century Oncology [USA]	2015.10.03	2016.03.10	2.2m		✓			
TalkTalk [UK]	2015.10.22	2015.10.22	4m	✓				
Nicchu Shinsei Corp [Japan]	2015.11.06	2016.03.26	18m	✓				
VTech [Hong Kong + Global]	2015.11.14	2015..11.27	11.6m+	✓				✓
US Voters Database [USA]	2015.12.28	2015.12.28	191m				✓	
UC Berkeley [USA]	2015.12.28	2016.02.29	80k+					✓

Business

Twelve major data breaches occurred in 2015 within the business sector. The Russian-based dating site, Topface, has been hacked in January 2015 exposing almost 20m logon credentials (BLI n.d.). AdultFriendFinder.com was hacked in May 2015. The site contains over 60m members worldwide of which 7m is based in the UK. Hackers have stolen millions of sensitive information records, of which almost 4m records were exposed. The type of data exposed includes users' sexual preferences and orientation, as well as users looking for swingers parties and extramarital affairs (White 2015). The extramarital affairs website, Ashley Madison, was hacked by the Impact Team hacker group in July 2015. This breach revealed financial records as well as 37m users' PII (Davis 2015). The largest theft of customer data from a USA financial institution occurred when JPMorgan was hacked in February 2015. Fifteen companies and more than 100m people were affected; more than 80% of the victims were from JPMorgan Chase. Three hackers involved have been charged (IdentityForce 2015). A hacker hacked into OOOwebhost, a free web hosting service, and dumped 13.5m records of PII, including passwords in plain text (BLI n.d.). Gaana.com suffered a massive data breach in May 2015 exposing over 10m users' PII. The attack was discovered and published only hours after the breach. Within one hour after discovery the vulnerability was patched (BLI n.d.). Wattpad, the world's largest readers and writer's community, experienced a data breach where 40m people's PII was compromised (BLI n.d.). In October 2015 a data breach on Experian, the world's biggest consumer credit monitoring firm, was disclosed. Since Experian processes T-Mobile's credit applications, T-Mobile was also affected. Fifteen million records containing sensitive personal information were exposed of individuals that applied for a credit check at T-Mobile between September 2013 and September 2015 (Ramanan 2015). TalkTalk, a UK based communications company, experienced a hack in February 2015, exposing over 150k customer's data. The total number of customers affected was 156,959, of which 15,656 customer's bank account numbers and sort codes were also hacked (Farrell 2015). In October 2015, TalkTalk were warned that all 4m customer's personal data may have been compromised (BLI n.d.). It was found that their database was left vulnerable to a SQL injection attack. This was TalkTalk's third breach and the second breach in 2015. In May 2016 it was reported that the company lost 100k customers due to the attack and cost more than £40m (including a £400k fine) to rectify (Glick 2015). Tokyo-based Nicchu Shinsei Corp was hacked in November 2015, where 18m login credentials were exposed. 1.78m of these belonged to customers of Yahoo Japan, Twitter, Facebook and Rakuten (BLI n.d.). VTech Holding, a Hong-Kong based company, announced that their learning Lodge database was compromised in December 2015, with 6.4m children and 4.9m parents' PII stolen. The customers affected were from the USA, France, UK, Germany and Canada (IdentityForce 2015).

Health/Medical

Four major data breaches occurred in 2015 within the health/medical sector. In February 2015, the largest data breach in healthcare history occurred when US based health insurer Anthem was breached. This breach disclosed 78.8m people's personal and employment information. No evidence was found of the stolen data being sold, shared or used fraudulently (Mathews 2015). UCLA Health System's network were compromised in July 2015 and hackers might have stolen 4.5million patients PII (IdentityForce 2015). The cancer care services company 21st Century Oncology revealed in March 2016 that their system was breached in October 2015, disclosing 2.2m patients' PII. No evidence showed that the stolen data has been used in any way (IdentityForce 2016). Personal information of over 90% of the 43m Korean population was sold after the Korea Pharmaceutical Information Center suffered a data breach (BLI n.d.).

Banking/Financial

Only one major data breach occurred in 2015 within the banking/financial sector. A data breach at the IRS was reported in June 2015 where criminals have stolen the tax returns of more than 100k people. It is believed that the attack originated from Russia. In August 2015 the IRS announced that 610k people have been affected by the breach (IdentityForce 2015). The number was again revised in February 2016, when they announced that the attack was much larger than initially alleged and that over 700k records were compromised (IdentityForce 2016).

Government/Military

Five major data breaches occurred in 2015 within the government/military sector. Turkish citizens' information was disclosed in clear text on the Internet in January 2015, exposing 49.6m+ personal records. Security loop holes were discovered, such as the use of a hardcoded password in the user interface, an unindexed database and weak encryption (Waqas 2016). OPM stated that the personal information of 22m citizens was compromised during a cyberattack in April 2015. 19.7m of the exposed data records were of individuals who applied for security clearances. The BSNL site was hacked by the hacker group AnonOpsIndia in July 2015. The data was not tampered with, but they warned the Indian government that the 30m+ exposed records is a goldmine for hackers (BLI n.d.). Hacking Team is an information technology company that develops spy tools for government agencies. In July 2015 a breach occurred where more than 1m emails were published, revealing the company's involvement with oppressive governments. It also revealed multiple Flash zero-day vulnerabilities, Adobe exploits and a full list of the company's customers. Most of the customers are military, police, federal and provincial governments (Ramanan 2015). A hacker named Phineas Fischer, who is believed to be behind this attack, were arrested in January 2017 (Khandelwal 2017). A security researcher discovered an incorrectly configured database on the Internet in December 2015, exposing 191 million USA voters' information (Finkle & Volz 2015).

Education

Two major data breaches occurred in 2015 within the education sector. VTech operates in both the business and education sectors (Refer to the breaches in the business section). More than 80k financial records from the University of California was compromised in December 2015 (made public in February 2016). The data exposed was of Berkeley students, alumni, employees and school officials (IdentityForce 2016).

3 Most Significant Data Breaches of 2016

The ITRC reported 980 data breaches in 2016 with 35,233,317 records disclosed. Figure 2 indicates that 44.1% of the breaches occurred in the business sector, 36.2 in the health/medical sector, 8.6% in the educational sector, 6.7% in the government/military sector and 4.4% in the banking/financial sector.

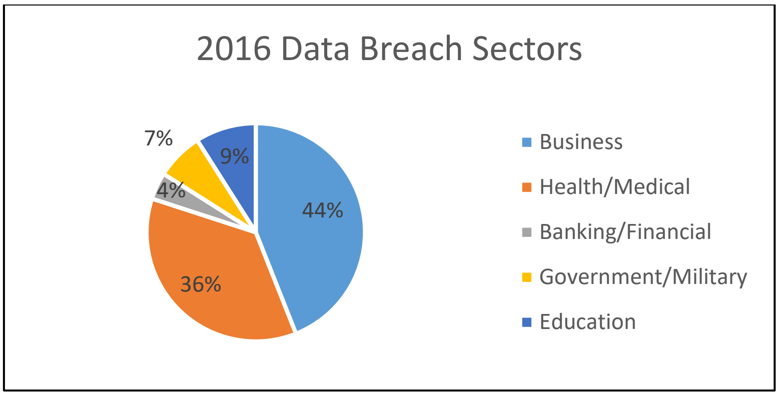

Figure 2. 2016 Data Breach Sectors (Compiled from ITRC n.d.)

Table 2 lists 22 of the most significant data breaches of 2016, sorted according to the breached date.

Table 2. Largest Data Breaches of 2016 (Compiled from IdentityForce 2016 and BLI n.d.)

Company / Agency [Country]	Breached Date	Published Date	Records Breached (Approx.)	Sectors				
				Business	Health/Medical	Banking/Financial	Government/Military	Education
Premier Healthcare [USA]	2016.01.15	2016.03.10	200k+		✓			
University of Central Florida [USA]	2016.01.31	2016.02.08	63k					✓
Weebly [USA]	01.02.2016	2016.10.20	43m+	✓				
Office of Child Support Enforcement [USA]	2016.02.09	2016.04.07	5m				✓	
Verticalscope [Canada]	2016.02.09	2016.06.13	45m	✓				
Mate1 [USA]	2016.02.16	2016.02.29	27m	✓				
Philippines Commission on Elections(COMELEC) [Philippines]	2016.03.28	2016.04.11	55m				✓	
Mossack Fonseca [Panama]	2016.03.31	2016.06.15	11.5m			✓		
JTB Corp [Japan]	2016.04.13	2016.06.14	7.9m+	✓				
Mexican Voters [Mexico]	2016.04.14	2016.04.22	93m+				✓	
17Media [Asia]	2016.04.29	2016.04.29	30m	✓				
MySpace [USA]	2016.05.##	2016.05.31	360m+	✓				
Interpark Corp [South Korea]	2016.05.05	2016.07.25	10m	✓				
Fling.com [UK]	2016.05.06	2016.05.06	40m	✓				
Turkish State Hospital [Turkey]	2016.05.18	2016.05.19	10m		✓			
Evony Gaming Company [USA]	2016.06.15	2016.10.##	33.4+m	✓				
Banner Health [USA]	2016.06.17	2016.08.03	3.7m		✓			
U.S. health insurer [USA]	2016.06.27	2016.06.27	9.3m		✓			
Mail.ru/Cross Fire/ParaPa-Dance-City/Ground-War-Tank [Russia]	2016.08.24	2016.08.24	25m+	✓				
U.S. Voter/Amazon/Google [USA]	2016.08.24	2016.08.24	25m+				✓	
Modern Business Solutions [USA]	2016.10.10	2016.10.10	58m	✓				
AdultFriendFinder [UK]	2016.10.16	2016.11.13	412.2m+	✓				

The sections below will discuss the data breaches presented in Table 2 in more detail, grouped according to sector.

Business

Twelve major data breaches occurred in 2016 within the business sector. In October 2016 Weebly discovered a breach, which occurred in February 2016, where 43m users' PII were stolen. No financial data were stolen and hackers were not able to log onto the websites due to the passwords being protected by bcrypt hashing (IdentityForce 2016). In June 2016, VerticalScope became aware of a data breach that happened February 2016, leaking more than 45m users' information online (BLI n.d.). A hacker gained access to over 27m plaintext passwords from Mate1.com in February 2016. He sold the data later with the asking price of 20bitcoins ($8700) (BLI n.d.). JTB Corp, Japan's biggest travel agency, suffered a hack in April 2016 that affected 7.93m people. The streaming app, 17Media, was hacked in April 2016, breaching 30m users' PII (BLI n.d.). A data breach was reported by MySpace in May 2016, leaking 360m account information records (IdentityForce 2016). Interpark Corp, an online shopping website from South Korea, was hacked in May 2016. This resulted in the leak of more than 10m customer data records (BLI n.d.). Fling.com was breached in May 2016 and 40m users' details were put up for sale on the Dark Web. Evony Gaming Company's website was hacked in June 2016, resulting in the theft of 33m gamer accounts. Three mail.ru communities were compromised in August 2016, leaking over 25m user records (BLI n.d.). Modern Business Solutions were hacked in October 2016 due to a poorly secured MongoDB database. The attackers dumped 58m records online (BLI n.d.). AdultFriendFinder.com was targeted again in October 2016; roughly 412m users' PII was compromised. The data was published on online criminal markets (IdentityForce 2016).

Health/Medical

Four major data breaches occurred in 2016 within the health/medical sector. Premier Healthcare reported a data breach in March 2016 where over 200k patients' sensitive data was compromised when a laptop was stolen from the billing department (IdentityForce 2016). The Turkish State Hospital experienced a breach in May 2016, where over 10m Turkish citizens' sensitive information were compromised (BLI n.d.). In August 2016, Banner Health reported that hackers gained unauthorised access to their computer systems that process the payment card data at food and beverage outlets. The attackers targeted approximately 3.7m payment card records. It was discovered that attackers might have also gained access to patient information, health plan information and information on physician and healthcare providers. The company reacted quickly to block the attackers and enhanced their security; fortunately not all Banner Health patients were affected by the attack. One year free membership were offered to patients who were affected by the attack (Banner Health 2016). An unnamed U.S. health insurer suffered a breach in June 2016 where 9.3m entries were up for sale on the dark web (BLI n.d.).

Banking/Financial

Only one major data breach occurred in 2016 within the financial sector. An IT worker of Mossack Fonseca, who have been arrested, was responsible for the leak of 11.5m financial records (BLI n.d.).

Government/Military

Four major data breaches occurred in 2016 within the government/military sector. In February 2016, external hard drives were stolen from the Office of Child Support in Washington by thieves who broke into their offices. The hard drives contained 5m records related to child-support audits. Two people have been arrested (BLI n.d.). COMELEC reported a breach on their database in March 2016, where all 55m voters in the Philippines's PII were compromised by Anonymous. It is said that the reason for the hack was to push COMELEC to strengthen security settings in the vote counting machines before the national elections (IdentityForce 2016). 93.4m Mexican voter's PII was compromised due to a misconfigured database. This data was uploaded to Amazon and exposed to the public (BLI n.d.). A database containing 154m voter profiles of US citizens was discovered by MacKeeper security researcher Chris Vickery. This was due to a database error. Unlike the previous the leaks on a US voters database that had been hosted by Amazon, this was hosted by Google (BLI n.d.).

Education

Just one major data breach was reported in 2016 within the education sector. The University of Central Florida had a breach that affected about 63k people (IdentityForce 2016).

4 Other Noteworthy Security Breaches

A number of security breaches occurred in 2015 and 2016 that has not necessarily resulted in exposed personal information at the time of writing this paper. The possibility exists that it can be exposed in the future, and as such these breaches will be briefly discussed in this section.

In July 2015, the pharmacy chain CVS had to shut down their online photo centre due to a security breach. An independent company hosting the CVSphoto.com website were hacked and credit card information might have been compromised. CVS notified all customers in time and no customers were affected (IdentityForce 2015). United Airlines suffered a data breach in June 2015 that resulted in the theft of flight manifests that included passengers' personal information. It is believed that the attack originated from the Chinese government and that it was the same hackers who was responsible for the Anthem and OPM data breach. In November 2015 it was reported that the Hilton Hotels were the victim of a security breach that affected guests at many of the 4500 hotels worldwide. Malware was found in the payment systems that gathered customer personal and financial information. (IdentityForce 2015).

In January 2016, the Austrian aircraft company, Fischer Advanced Composite Components, reported a major cyber-attack with a loss of $54m. The company had an immense fall in share price, reputational damage and a big cost of remediation and recover, resulting in a much higher overall cost of the breach (Ashford 2016; IdentityForce 2016). In January 2016 a Distributed Denial of Service attack on the election campaign website of Donald Trump (Donaldjtrump.com), the newly elected president of the USA in 2017, was executed by a hacking group called New World Hacktivists (NWH). This group also attacked BBC websites in 2015 (Tagade 2016). In a separate attack, Hillary Clinton's campaign was also hacked exposing 19k emails from the Democratic National Committee (DNC) (Conger 2016). The AnonSec Collective hacker group broke into the NASA computer systems in January 2016, stealing footages of a fleet aircraft, data logs as well and personal information of more than 2400 employees (Tagade 2016). In February 2016, CNN reported that 10k employee data records from Homeland Security and 20k FBI employee data records were exposed. This attack was executed by hackers that were angry about the US relations with Israel. It took the Department of Justice one week to realise the breach (IdentityForce 2016). In June 2016, Facebook's CEO Mark Zuckerburg's Twitter and Pinterest accounts were hijacked. He reused the password "dadada", which was exposed in the 2012 LinkedIn hack, on these websites (Mcmillan 2016). Yahoo announced in December 2016 that another data breach was discovered from 2013, less than three months after announcing a data breach from 2014. The 2014 breached exposed 500m Yahoo users' credentials; the 2013 breach exposed over 1b Yahoo account information records. This is the largest known data breach in history (IdentityForce 2016). LinkedIn was hacked in 2012, when 117m logon credentials were stolen. This data only became publicly available in May 2016. Dropbox, one of the popular cloud storage services, was challenged with a data breach that was made public in September 2016. This breach, which occurred in 2012 already, revealed more than 68m user's credentials (IdentityForce 2016). The Municipal Transportation Agency of San Francisco was infected with malware in November 2016. This attack caused the systems to lock down, allowing passengers free rides for two days. It was discovered that it was not a targeted attack but an automated attack (known as spray and pray). One of the IT administration personnel clicked on a link that downloaded malware without the person realising it. The hackers stole 30GB of data, including PII of employees and customers, and demanded the security fixing of the vulnerability and the payment of 100 Bitcoins (about $73,000). The hackers threatened to release the information if the demands were not met. The system was back online within two days, but no evidence showed that the hackers have been paid (IdentityForce 2016). Tesco Bank, from the UK, had a data breach in November 2016 where 9,000 customer accounts were affected and approximately £2.5m were stolen. This is the biggest cyber-heist of its kind in the UK (Leydon 2016).

5 Comparative Review of the Data Breaches

An independent comparative review was conducted by the authors based on the significant data breaches presented in Table 1 and Table 2. This review is done to identify whether the general trend remains the same regardless of whether the data breach result in PII leakage. Sections 2 and 3 introduced a number of significant data breaches that occurred in 2015 and 2016. Based on the pie graphs presented (refer to Figure 1 and Figure 2 for the percentage of data breaches reported), it is clear that the business sector is by far the most targeted, with 40% and 44% of all reported breaches respectively for 2015 and 2016. A number of reasons exist for this, such as non-adoption of the latest security measurements, or implementation errors by companies who do adopt security measures, leaving them vulnerable to new type of attacks (Experian Inc 2016). The health/medical sector is the second most targeted, with 36% of all reported breaches for both years. The health sector faces the most costly data breaches and it is forecasted that the cost will rise annually due to potential economic gain and digitisation of records. Medical records are worth in excess of 10 times more than credit card information on the black market (Experian Inc 2016). Many argue that the health sector is not up to standard with securing information (Della Costa 2015). The other sectors vary between 4% and 9%.

Table 3 presents an overview of the number of data breaches and the resultant number of exposed records based on the selected significant data breaches presented in Table 1 and Table 2. Table 3 shows that the business sector is the most targeted for data breaches with resultant PII record leakage, with 50% and 55% of all reported breaches for 2015 and 2016 respectively. The amount of records breached in 2016 is significantly higher than 2015 with over 1b records breached in the business sector alone. The government/military was the second most targeted in terms of reported breaches, with 21.7% in 2015 and 18% in 2016. This sector is also second in terms of PII record leakage. The health/medical sector is the third most targeted in terms of PII record leakage and reported breaches, with 17.4% in 2015 and 18% in 2016. In terms of significant reported breaches, the banking/financial sector was targeted 4.4% and the educational sector 6.5% in 2015. The banking/financial and education sectors are equally targeted in terms of significant breaches in 2016, at 4.5%. In previous years the financial industry was highly targeted but this has decreased, arguably as a result of newly implemented policies, protocols and procedures. An annual decline has also been observed in the education sector, arguably as a result of the focus shifting to more lucrative targets such as the business and healthcare industries (Trend Micro 2015).

Table 3. Significant Breaches & Number of Breached Records: 2015 & 2016 (Refer to Tables 1 & 2)

Sector	Significant Reported Breaches		Breached Records (Approx.)	
	2015	2016	2015	2016
Business	50%	55%	273.2m+	1.09b+
Health/Medical	17.4%	18%	128.5m+	23.2m+
Banking/Financial	4.4%	4.5%	700k+	11.5m+
Government/Military	21.7%	18%	293.6m+	178m+
Education	6.5%	4.5%	11.6m+	63k+

Where an organisation is linked to more than one sector, the weight is divided equally between sectors

If the compromised PII records mentioned in Section 4 were to be exposed, it would have a significant effect on the statistics shown in Table 3. Many of these noteworthy breaches are in the business and government/military sectors and as such would have a major impact on these particular areas.

Figure 3 presents the percentage of significant data breaches per month for 2015 and 2016. Note that these breaches are only applicable to the data in Table 1 and Table 2. The most data breaches in 2015 occurred in May (19%) and June (25%). In 2016 the most breaches occurred in February (17%) and May (17%). Towards the end of 2015 a number of major data breaches occurred, whereas in 2016 no major breaches occurred after October. In terms of trending data breaches per country, the significant data breaches discussed in Sections 2 and 3 show a significant majority of data breaches (48% in both 2015 and 2016) occurring in the USA. This could be due to the fact that the data sources that collected the data is based in the USA and thus focus more on breaches within the USA. It could also be that a big part of the largest companies in the world are based in the USA and therefore are targeted more than other countries. The data breaches in other countries were almost equally divided between the UK, European countries and Asia.

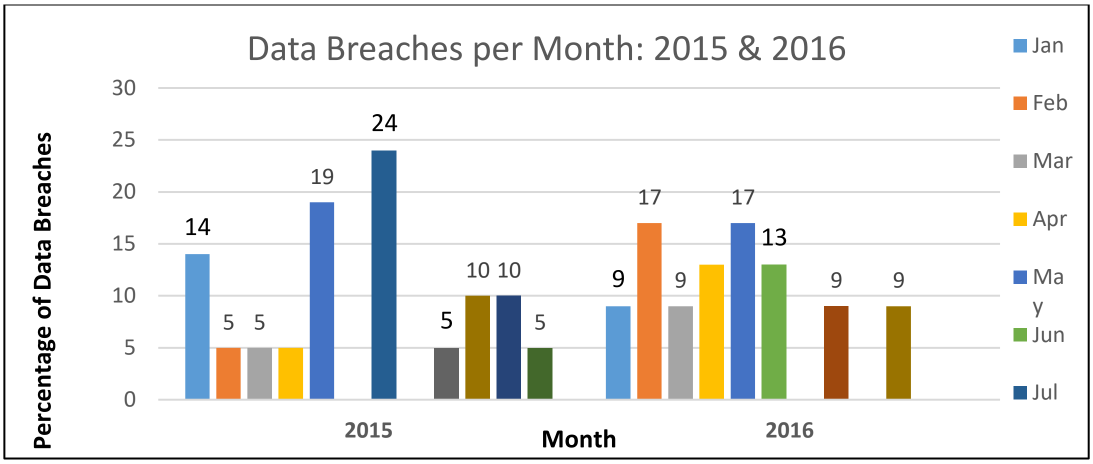

Figure 3. Data Breaches per Month: 2015 & 2016

Based on the Breach Level Index (BLI n.d.), the biggest data breach in 2015 was the Anthem breach (with a risk score of 10). The Turkish Citizenship Database (9.9) was second and the Ashley Madison (9.8) breach third. The biggest breach in 2016 was AdultFriendFinder.com (10), followed by Fling.com (9.8) and 17Media (9.7).

6 Conclusion

Cybercriminals continue to identify vulnerabilities and loopholes in networks and systems to gain access to networks and conduct data breaches. Data breaches have gained extensive coverage as businesses and organisations of all sizes become more dependent on the digital domain. The aim of this paper was to highlight the most significant data breaches from 2015 and 2016, with special references to PII leakage. 2015 has seen some of the world's largest recorded data breaches. In 2016 there were less breaches overall, but the amount of breached records were significantly higher than 2015. The breaches were grouped according to the sectors that they operate in to determine which sectors were affected the most. It was discovered that the business sector is affected the most by far, trailed by the government/military sector. The health industry is targeted more and more in recent years. A decline has also been observed in the education sector over the last few years, arguably as a result of the focus shifting to more lucrative targets such as the business and healthcare industries. Based on the findings in this study and previous studies it can be stated that cybercrime and security is an ongoing battle internationally and can no longer be dismissed. The vulnerability of online systems and the potential for economic loss as a result of PII leakage is a very significant threat.

References

Ashford, W., 2016. $54m cyber fraud hits aircraft supplier share price. Available at: http://www.computerweekly.com/news/4500271523/54m-cyber-fraud-hits-aircraft-supplier-share-price [Accessed January 17, 2017].

Banner Health, 2016. Banner Health Identifies Cyber Attack | Banner Health. Available at: https://www.bannerhealth.com/news/2016/08/banner-health-identifies-cyber-attack# [Accessed January 14, 2017].

BLI, Data Breach Statistics. *Breach Level Index*. Available at: http://breachlevelindex.com/ [Accessed February 6, 2017].

Conger, K., 2016. Clinton campaign breached by hackers. *TechCrunch*. Available at: https://techcrunch.com/2016/07/29/clinton-campaign-reportedly-breached-by-hackers/ [Accessed January 29, 2017].

Della Costa, C., 2015. Why Health Care Faces the Most Costly Data Breaches. *The CheatSheet*. Available at: http://www.cheatsheet.com/business/this-industry-faces-the-mostly-costly-data-breaches.html/?a=viewall [Accessed February 3, 2017].

Davis, J., 2015. 7 Largest Data Breaches of 2015. *Healthcare IT News*, p.1. Available at: http://www.healthcareitnews.com/news/7-largest-data-breaches-2015.

Experian Inc, 2016. Data Breach Industry Forecast. , pp.1–29. Available at: http://www.experian.com/assets/data-breach/white-papers/2016-experian-data-breach-industry-forecast.pdf.

Farrell, S., 2015. Nearly 157,000 had data breached in TalkTalk cyber-attack. Available at: https://www.theguardian.com/business/2015/nov/06/nearly-157000-had-data-breached-in-talktalk-cyber-attack

[Accessed April 18, 2017].

Finkle, J. & Volz, D., 2015. Database of 191 million U.S. voters exposed on Internet: researcher | Reuters. Available at: http://uk.reuters.com/article/us-usa-voters-breach-idUKKBN0UB1E020151229 [Accessed January 14, 2017].

FreedomidDirect, What Identity Thieves Want - Your Personal Identifiable Information. Available at: https://freedomiddirect.com/pages/what-identity-thieves-want [Accessed January 27, 2017].

Glick, B., 2015. TalkTalk hit by record £400,000 fine over data breach. *ComputerWeekly.com*. Available at: http://www.computerweekly.com/news/450400451/TalkTalk-hit-by-record-400000-fine-over-data-breach [Accessed January 27, 2017].

IdentityForce, 2016. 2016 Data Breaches | IdentityForce. Available at: https://www.identityforce.com/blog/2016-data-breaches [Accessed January 28, 2017].

IdentityForce, 2015. The Biggest Data Breaches in 2015. Available at: https://www.identityforce.com/blog/2015-data-breaches [Accessed January 30, 2017].

ITRC, ID Theft Resource Center 888-400-5530. Available at: http://www.idtheftcenter.org/ [Accessed January 14, 2017].

Khandelwal, S., 2017. Police Arrested Suspected Hacker Who Hacked the “Hacking Team.” *The Hacker News*. Available at: http://thehackernews.com/2017/01/phineas-fisher-hacking-team.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.1419.au0ao0accb.u8c [Accessed February 3, 2017].

Kuranda, S., 2015. The 10 Biggest Data Breaches Of 2015 (So Far) - Page: 2 | CRN. Available at: http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm/pgno/0/1 [Accessed January 15, 2017].

Leydon, J., 2016. “Tesco Bank”s major vulnerability is its ownership by Tesco,’ claims ex-employee. *The Register (UK)*. Available at: http://www.theregister.co.uk/2016/11/30/tesco_bank_breach_former_insider_breach_theory/ [Accessed January 30, 2017].

Mathews, A.W., 2015. Anthem: Hacked Database Included 78.8 Million People - WSJ. Available at: http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364 [Accessed January 14, 2017].

McCoy, K., 2016. Cyber hack got access to over 700,000 IRS accounts. *USA TODAY*. Available at: http://www.usatoday.com/story/money/2016/02/26/cyber-hack-gained-access-more-than-700000-irs-accounts/80992822/ [Accessed January 28, 2017].

Mcmillan, R., 2016. Mark Zuckerberg’s Twitter and Pinterest Accounts Hacked. *The Wall Street Journal*. Available at: http://www.wsj.com/articles/mark-zuckerbergs-twitter-and-pinterest-accounts-hacked-1465251954 [Accessed January 28, 2017].

oecd.org, 2013. *THE OECD PRIVACY FRAMEWORK* OECD Council, ed., OECD.

Paganini, P., 2015. Cybercrime exploits Anthem data breach in Phishing campaigns. , 2015(Sep/24). Available at: http://securityaffairs.co/wordpress/33278/cyber-crime/anthem-phishing-campaigns.html.

Privacy Rights Clearinghouse, Data Breaches. Available at: https://www.privacyrights.org/data-breaches [Accessed January 30, 2017].

Ramanan, S., 2015. What are the top 10 Cyber security breaches of 2015? - Quora. Available at: https://www.quora.com/What-are-the-top-10-Cyber-security-breaches-of-2015 [Accessed January 15, 2017].

Romanosky, S., 2011. Do Data Breach Disclosure Laws Reduce Identity Theft ? *Journal of Policy Analysis and Management*, 30(2), pp.256–286. Available at: http://onlinelibrary.wiley.com/doi/10.1002/pam.20567/epdf.

Tagade, K., 2016. What are the top 10 Cyber security breaches of 2016? Available at: https://www.quora.com/What-are-the-top-10-Cyber-security-breaches-of-2016 [Accessed January 28, 2017].

Trend Micro, 2015. Follow the Data : Analyzing Breaches by Industry.

Waqas, 2016. Someone Hacked and Leaked Entire Turkish Citizenship Database Online. Available at: https://www.hackread.com/turkish-citizenship-database-hacked-leaked/ [Accessed January 14, 2017].

Weise, E., 2016. Top hacks and data breaches. *USAToday*. Available at: https://www.usatoday.com/story/tech/news/2016/12/14/biggest-data-breaches/95446624/ [Accessed April 18, 2017].

White, G., 2015. Adult dating site hack exposes millions of users. Available at: https://www.channel4.com/news/adult-friendfinder-dating-hack-internet-dark-web [Accessed January 27, 2017].