2015

The Year Data Breaches Got Personal

Findings from the 2015

BREACH LEVEL INDEX

POWERED BY

gemalto

security to be free

BREACH LEVEL INDEX

THE NUMBERS

> *More and more organizations are accepting the fact that, despite their best efforts, security breaches are unavoidable.*

RECORDS BREACHED IN THE YEAR 2015

707,509,815

NUMBER OF BREACH INCIDENTS

1,673

NUMBER OF BREACHES WITH OVER 1 MILLION RECORDS AFFECTED

46

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

47%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

EVERY DAY
1,938,383

EVERY HOUR
80,766

EVERY MINUTE
1,346

EVERY SECOND
22

INTRODUCTION

2015 YEAR IN REVIEW

In 2015, data breaches got much more personal than in previous years. While cybercriminals made headlines stealing credit card data and financial information in 2013 and 2014, the theft of personal information and identities took center stage in 2015. In fact, this type of theft accounted for 53% of all data breaches last year.

Perhaps the best thing one can say about 2015—from a data breach standpoint—is that it wasn't 2014. The prior year was historic in terms of big, high-profile data breaches and a number of lesser-known attacks that resulted in the theft of more than one billion data records.

That's not to say 2015 was easy for information security and IT executives—not by a long shot. The year had its own share of highly publicized and damaging attacks, and these incidents continued to keep cyber security in the headlines. In fact, there were 46 data breaches that involved the loss or theft of one million or more data records.

2015 Key Findings

According to data collected in the **Breach Level Index (BLI),** there were 1,673 reported data breaches in 2015, which resulted in more than 707.5 million records being compromised worldwide. Compared to 2014, the total number of data breaches actually declined by 3.4% and the total number of compromised records dropped by 39%.

Malicious outsiders accounted for 58% of all data breaches – more than any other source. The theft of personal information and identities lead all other types of data theft, accounting for 53% of all data breaches. The healthcare industry led all sectors, accounting for 22% of all data breaches. However, government accounted 43% of all lost or stolen data records, more than any other industry sector.

From a time perspective, in 2015 some 1,938,383 data records were stolen or lost every day, 80,766 every hour, 1,346 every minute and 22 every second. So, in the time it took to read the previous sentence, about 400 data records would have been stolen or lost.

Another interesting statistic is that of all the data breaches in 2015, 47% of them had an unknown number of compromised records, demonstrating that the actual number of compromised records is actually understated.

And despite the growing interest of encryption technology as a means to protect for information and privacy, only 60 of the reported data breach incidents in 2015, or less than 4% of the total, involved data that was encrypted in part or in full.

To create this report, **Gemalto**, a leading global provider of digital security solutions, has collected extensive publicly-available information about data breaches around the world. The information is aggregated in the Breach Level Index, a database Gemalto maintains on data breaches globally.

The report analyzes the data in terms of the number of breaches, the number of data records lost, and data breaches by industry, type of breach, source of the breach and by country or region.

DATA BREACHES

The one dominant characteristic of data breaches in 2015 was how much more personal they have become. The targeting of individuals' identities and their personal information such as the data breaches involving the U.S. Office of Personnel Management, Anthem Insurance, and Experian exposed just how valuable this information has become to cybercriminals. While credit cards have built in security mechanisms that limit the exposure and risk for individuals if they are stolen, theft of personally identifiable information is something totally different as more damage can be done with stolen identities and they are also more difficult to recover.

While 2015 might not have had as many headline-grabbing data breaches as the previous year, it certainly saw a continuation of the large-scale assaults that have made cyber security a top priority for senior business executives and boards of directors at many companies. And what makes the large-scale data breaches of 2015 somewhat disconcerting is that they came despite the fact that so many enterprises are supposedly bolstering their defenses in response to previous high-profile breaches.

Each of the five biggest breaches of the year resulted in the exposure of huge amounts of personal information and identities. The most severe breach of 2015, which received the highest possible score in terms of severity on the BLI, was an identity theft attack on Anthem Insurance. Other top breaches affected organizations including Turkey's General Directorate of Population and Citizenship Affairs, Korea's Pharmaceutical Information Center, the U.S. Office of Personnel Management and Experian.

> The targeting of **individuals' identities** and their **personal information** exposed just how valuable this information has become to cybercriminals.

Since the Breach Level Index began tracking publicly disclosed data breaches in 2013, more than 3.6 billion data records have been exposed. Surely the massive volumes of data theft reflects the fact that more information than ever is available for exposure, including data from mobile devices, online digital transactions, social media and other sources. Never before has so much personally-identifiable information been available for potential theft.

Following are some of the most noteworthy examples of data breaches in 2015, including the number of records stolen, type of breach and BLI risk assessment score. The score is calculated based on such factors as the total number of records exposed, the type of data within the records, the source of the breach and how the information was used.

A BLI score of 1 to 2.9 is classified as a minimal risk, 3 to 4.9 is moderate, 5 to 6.9 is critical, 7 to 8.9 is severe and 9 to 10 is catastrophic. The idea behind the scoring system in the BLI is to demonstrate that not all breaches have the same impact on organizations or the same amount of risk.

TOP SCORING BREACHES

2015 YEAR IN REVIEW

Anthem Insurance

Records: **78,800,000**
Type: **Identity Theft**
Score: **10.0**

The attack against U.S.-based health insurer Anthem was an identity theft breach that resulted in the theft of 78.8 million records, making it the largest data breach of the year in terms of records compromised. The breach scored a 10 on the risk assessment scale. The company issued a statement saying that in January it had learned of a cyber attack on its IT system, and that cyber attackers tried to get private information about individuals with data on Anthem systems. Current and former members of one of Anthem's affiliated health plans, as well as some members of other independent Blue Cross and Blue Shield plans who received healthcare services in any of the areas that Anthem serves, were said to be affected. Investigators suspected that the hack that lead to this breach was sponsored by a foreign state.

General Directorate of Population and Citizenship Affairs

Records: **50,000,000**
Type: **Identity Theft**
Score: **9.9**

The Turkish government agency experienced an identity theft attack at the hands of a malicious outsider. The attack exposed 50 million records and scored a 9.9 on the scale. The Presidency's State Audit Institution (DDK) reported that the servers supporting the administration's Web site were breached and information pertaining to citizens was stolen.

Korea Pharmaceutical Information Center

Records: **43,000,000**
Type: **Identity Theft**
Score: **9.7**

The South Korean organization, which distributes pharmacy management software to many of the country's pharmacies, was hit by an identity theft breach launched by a malicious insider. The result was the exposure of 43 million records, and the incident scored a 9.7 on the risk assessment scale. According to the Korea Herald, medical information on nearly 90% of the South Korean population was sold to a multi-national firm, which processed and sold the data.

U.S. Office of Personnel Management (OPM)

Records: **22,000,000**
Type: **Identity Theft**
Score: **9.6**

The OPM in June 2015 suffered an identity theft data breach that involved 22 million records. The state-sponsored attack, which was described by federal officials as being among the largest breaches of government data in the history of the U.S., scored a 9.6 on the risk assessment scale. The attack exposed data including personally identifiable information such as Social Security numbers, names, dates and places of birth, and addresses.

Experian

Records: **15,000,000**
Type: **Identity Theft**
Score: **9.4**

The U.S.-based credit bureau and consumer data broker experienced an identity theft breach by a malicious outsider that resulted in the theft of 15 million records. The attack, which the company disclosed in October 2015, scored 9.4 on the risk assessment scale. Experian North America, in a news release, said one of its business units experienced an unauthorized acquisition of information from a server that contained data on behalf of one of its clients, T-Mobile USA. The data included some personally identifiable information about consumers in the U.S., including those who applied for T-Mobile services or device financing.

LEADING SOURCES OF DATA BREACHES

A key part of defending against cyber security attacks is knowing who the adversaries are and what tactics they used. Armed with this knowledge, organizations can at least take steps to mitigate future risk of attack or loss of data.

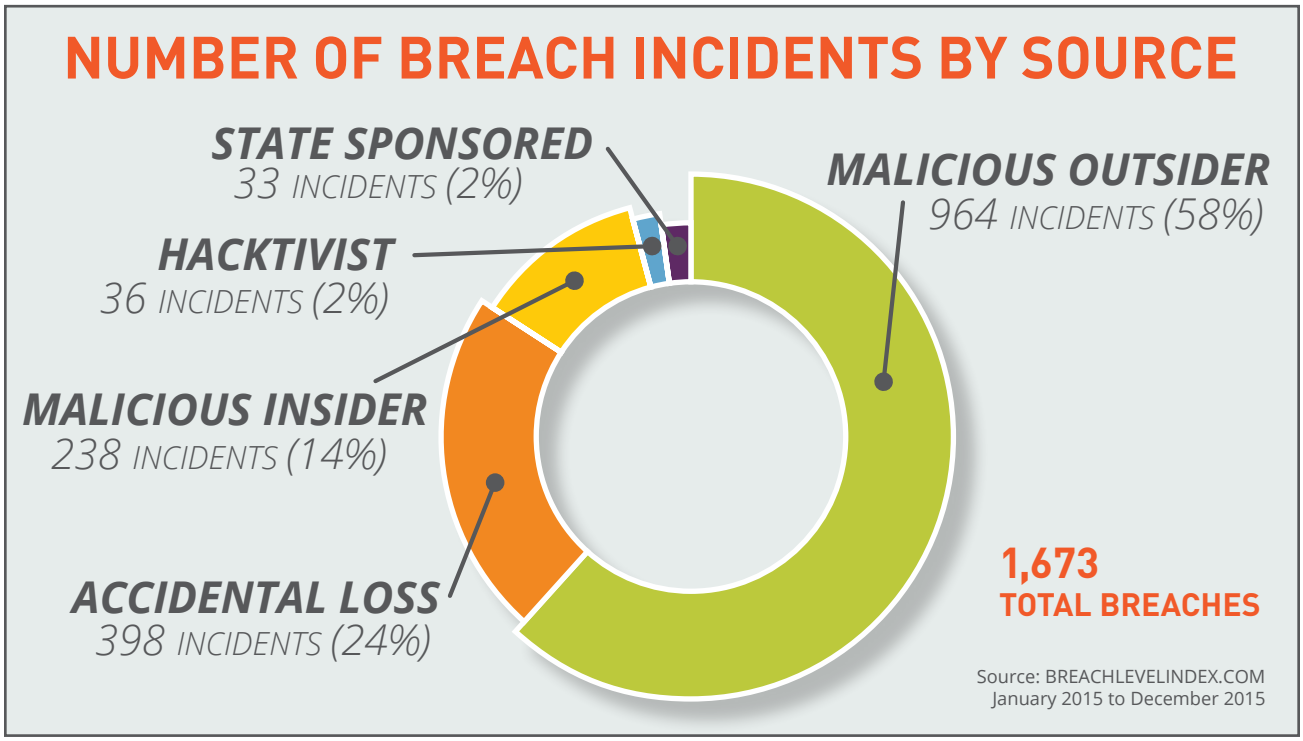
In 2015 the leading source of data breaches was **malicious outsiders**, accounting for 964 attacks, or 58% of the total. Those figures are actually up slightly from the year before, when malicious outsiders were also the number one source of breaches. Attacks by these cybercriminals exposed more than 265.2 million records, or 37% of the total, in 2015.

While malicious outsiders accounted for the biggest percentage of data breach incidents, **accidental loss** of data records accounted for 36% of all records lost (257.7 million) due mainly to the United States government's loss of more than 191 million voter records. Accidental loss accounted for the second largest number of breaches with 398, or 24% of the total.

Next among the sources of attacks were **malicious insiders**, who launched 238 attacks (14%). These attacks exposed 46.3 million records (7%).

Hacktivists were next on the list, conducting 36 attacks (2.1% of the total), which accounted for 30.6 million records exposed (4%). While this is still a relatively small portion of the overall breaches, it represents are fairly significant jump from 2014, when hactivists launched only 20 attacks that affected 8.2 million records.

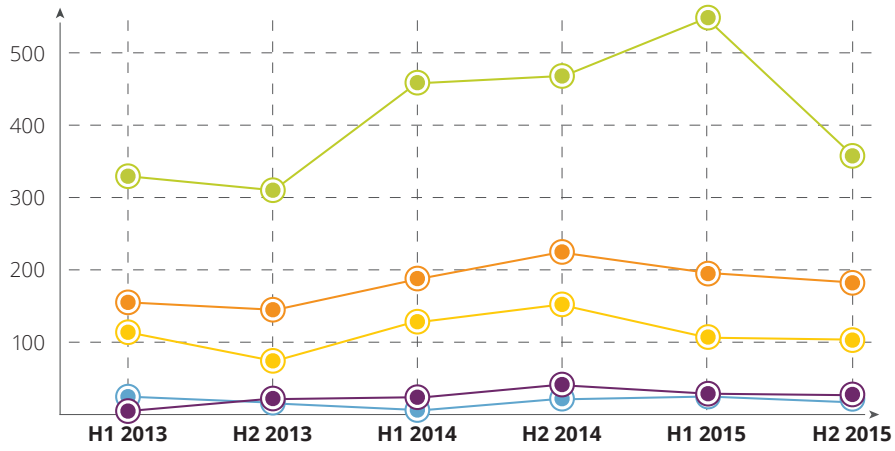
State-sponsored attacks totaled 33 in 2015, for 2% of the total. These breaches involved 107.7 million records (15%). It's notable that the number of records is fairly high given the relatively low number of state-sponsored breaches.



DATA BREACHES BY SOURCE OVER TIME

2015 YEAR IN REVIEW

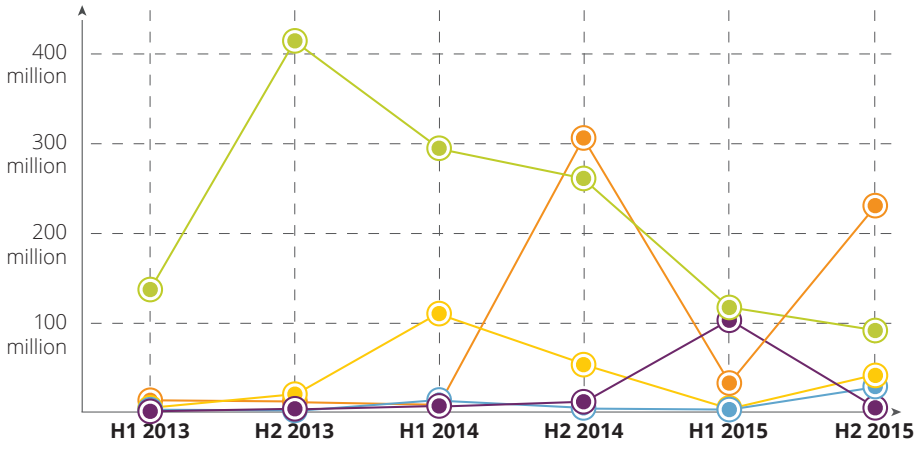
NUMBER OF BREACH INCIDENTS BY SOURCE OVER TIME



SOURCE	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015
Malicious Outsider	335	314	465	470	546	365
Accidental Loss	159	140	189	216	197	179
Malicious Insider	114	78	125	153	107	101
Hacktivist	21	8	4	15	19	18
State Sponsored	3	10	20	40	17	14

Source: BREACHLEVELINDEX.COM

NUMBER OF RECORDS BREACHED BY SOURCE OVER TIME



SOURCE	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015
Malicious Outsider	142,693,717	409,067,412	297,681,964	263,311,253	114,520,847	90,116,661
Accidental Loss	8,482,892	6,140,675	3,425,588	305,285,159	28,568,633	229,087,967
Malicious Insider	1,149,769	9,200,723	106,190,172	52,947,689	784,329	44,401,906
Hacktivist	777,216	98,730	7,000,096	1,182,005	561,918	30,011,904
State Sponsored	38	165,015	3,016,499	6,912,064	102,883,225	4,067,411

Source: BREACHLEVELINDEX.COM

TYPES OF DATA COMPROMISED

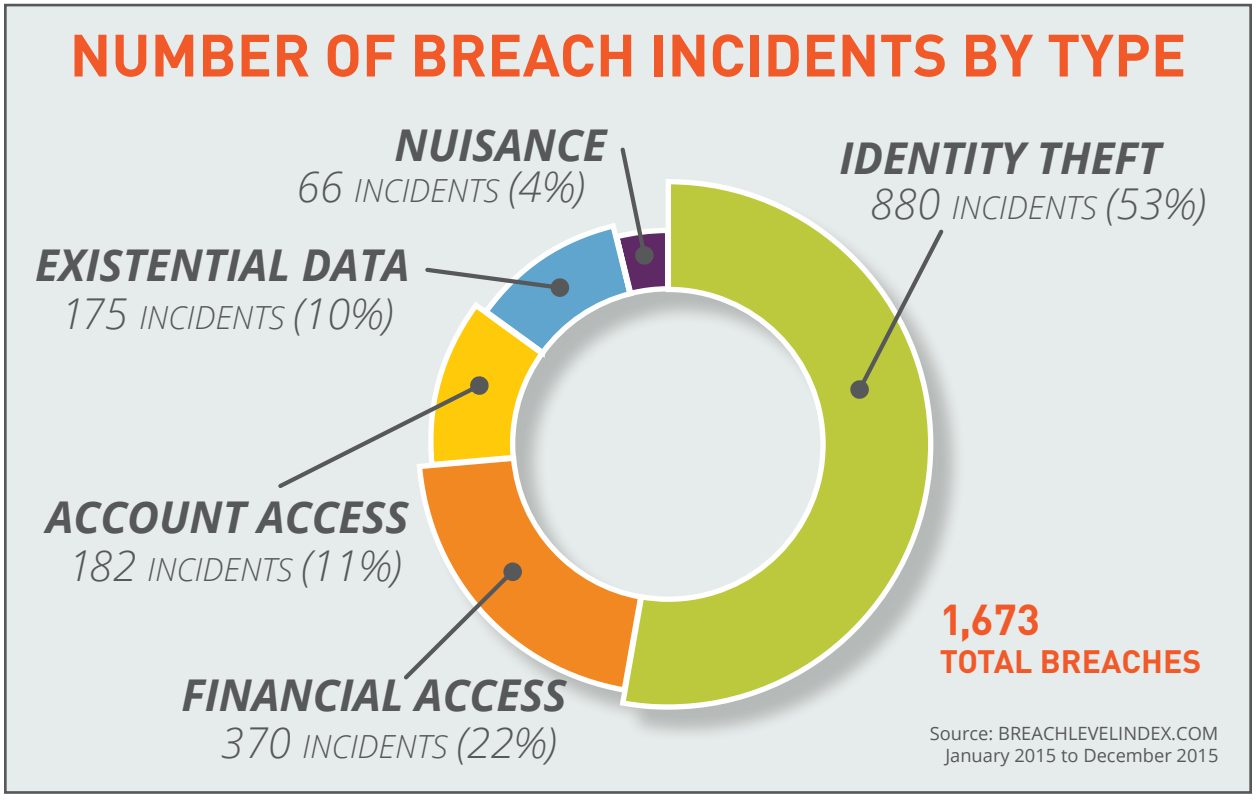
As in past years, attackers used a variety of methods to conduct major data breaches in 2015. At the top of the list for the second straight year was identity theft, which was easily the most common type of breach.

Identity theft breaches accounted for nearly half (40%) of all records compromised during the year, with a total of 285 million. These types of attacks accounted for slightly more than half (53%) of all data breaches, with 880. If security executives needed further evidence that identity theft is a still a serious problem, this is it.

The next most common type of data breach was **financial access** data theft, which was used in 370 of the attacks and accounted for 22% of the total. Interestingly, financial data theft incidents exposed only 5.7 million records, which accounted for a tiny fraction (less than 1%) of the total.

Account access was next on the list of breach types, with 182 breaches (11% of the total) and 102.5 million records (14.5%).

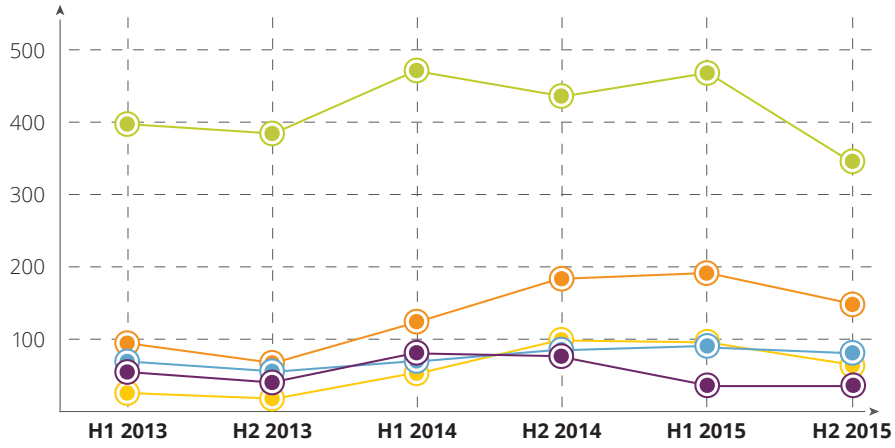
This was followed by **existential data**, with 175 attacks (11%) and 107.8 million records (15%); and **nuisance** attacks, with 66 attacks (4%) and 206.5 million (29%). The last category exposed a startling number of records considering there were comparatively few attacks.



DATA BREACHES BY TYPE OVER TIME

2015 YEAR IN REVIEW

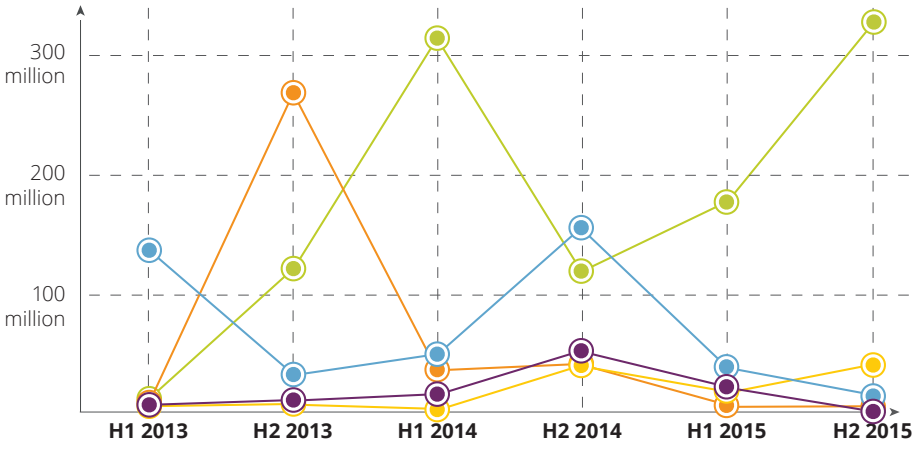
NUMBER OF BREACH INCIDENTS BY TYPE OVER TIME



TYPE OF BREACH	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015
Identity Theft	396	382	474	443	472	350
Financial Access	97	71	119	183	197	150
Existential Data	25	13	54	98	96	63
Account Access	76	52	74	92	93	86
Nuisance	55	35	86	81	30	30

Source: BREACHLEVELINDEX.COM

NUMBER OF RECORDS BREACHED BY TYPE OVER TIME



TYPE OF BREACH	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015
Identity Theft	6,436,318	121,624,113	316,003,444	115,316,845	185,717,096	330,695,763
Financial Access	4,060,027	270,264,132	34,905,015	35,876,605	2,071,434	2,656,283
Existential Data	1,818,066	3,323,008	555,843	35,573,128	8,784,671	46,539,303
Account Access	138,226,695	23,375,563	50,911,957	156,442,510	34,315,208	17,654,815
Nuisance	2,635,306	6,090,484	14,939,907	50,882,682	15,030,984	140,182

Source: BREACHLEVELINDEX.COM

COMPARING THE INDUSTRIES

It appears that **government organizations** were among the new favorite targets of hackers and other attackers. Agencies and other public sector entities accounted for nearly half of all compromised data records (43%), up an astounding 476% from 2014.

This was due to several extremely large data breaches in the United States and Turkey. The total number of attacks in the government sector was 272 (16%), involving

307.1 million

records. The average number of records exposed per attack was more than 1,129,000, compared with about 190,000 in 2014.

The **healthcare** industry was also hit fairly hard in 2015. The sector accounted for 19% of total records compromised (134 million). As with the government, the number of records exposed rose dramatically compared with the year before, with a whopping 217% increase.

The total number of breaches in the industry during the year was

374

- 22% of all breaches and the highest number of any sector. The results clearly show that a sector that places a high level of importance on the protection and privacy of information needs to work harder to keep data safe from intruders.

The **retail** sector saw a big drop (-93%) in the number of stolen records compared with 2014. The total number of records affected was 40.1 million, accounting for just under 6% of stolen records.

The 217 data breaches in the industry accounted for 13% of the total number of breaches in 2015. What stands out with this sector is that even though there were more breaches in 2015 than the year before, the number of records stolen was down drastically in the same period.

The **financial services** sector also saw a huge drop in records stolen (down 99%), even though the number of breaches went up. The 1.1 million records represented just 0.1% of compromised data records in 2015.

Finance companies experienced 253 breaches during the year, or 15% of the total.

The **education** sector saw a relatively low number of breaches and records stolen, compared with other industries. Educational institutions experienced a total of 150 breaches, accounting for 9% of the total. The number of records exposed was 19.3 million, or 3%.

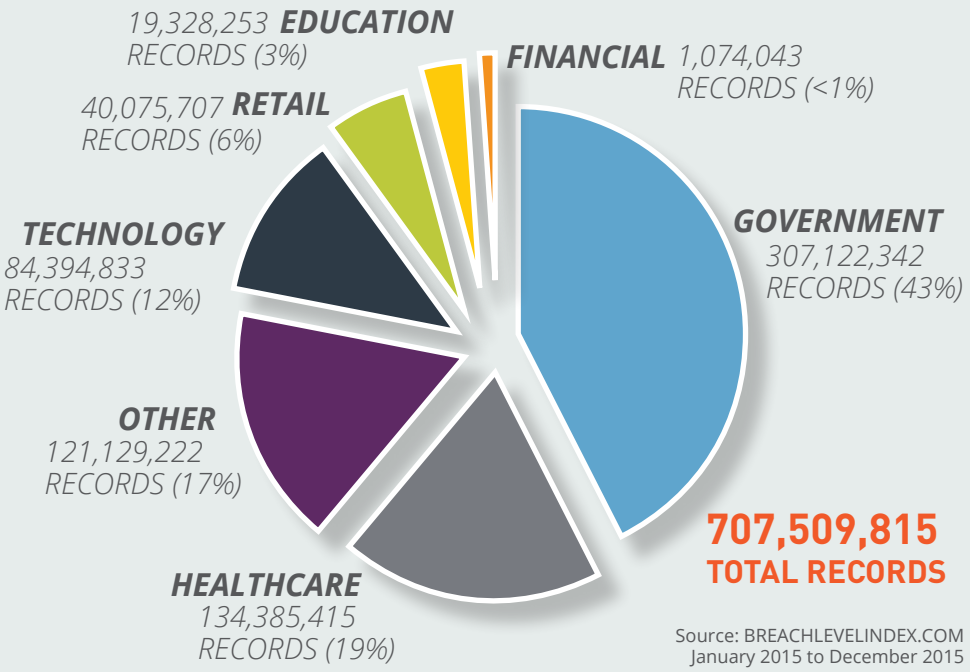
COMPARING THE INDUSTRIES

2015 YEAR IN REVIEW

TECHNOLOGY

As with education, the **technology** industry was apparently not as highly targeted as other industries in 2015. The sector had 104 data breaches, accounting for just 6.2% of the total. But the number of records exposed, 84.4 million, accounted for 12% of the total.

NUMBER OF RECORDS BREACHED BY INDUSTRY IN 2015



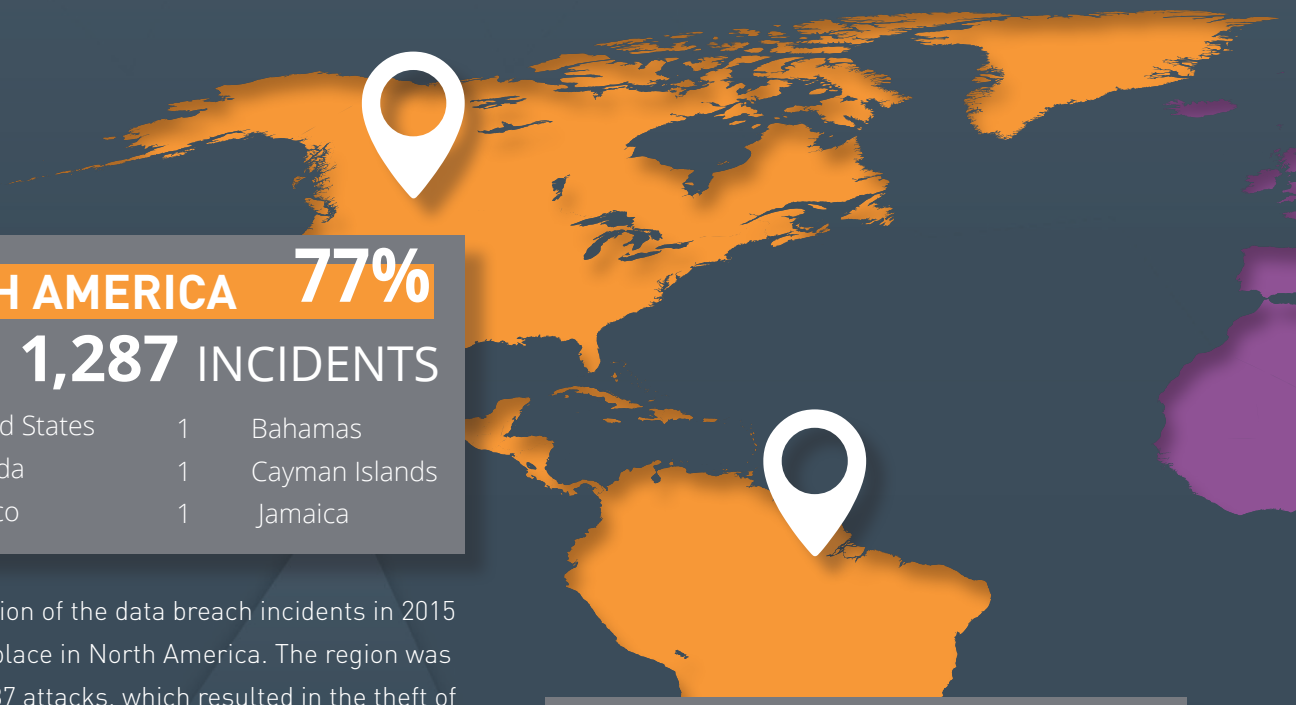
Source: BREACHLEVELINDEX.COM
January 2015 to December 2015

NUMBER OF BREACH INCIDENTS BY INDUSTRY OVER TIME

INDUSTRY	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015
Healthcare	172	168	236	200	186	159
Financial Services	79	87	85	125	143	101
Government	128	65	108	182	142	114
Retail	58	42	83	112	115	87
Education	7	26	88	84	94	50
Technology	56	54	72	65	47	48
Other Industries	151	113	142	131	161	120

Source: BREACHLEVELINDEX.COM

THE GEOGRAPHICAL VIEW



NORTH AMERICA 77%

1,287 INCIDENTS

1,222	United States	1	Bahamas
59	Canada	1	Cayman Islands
3	Mexico	1	Jamaica

A large portion of the data breach incidents in 2015 (77%) took place in North America. The region was hit with 1,287 attacks, which resulted in the theft of 460.6 million records (65% of the total). The number of breaches rose 11% from 2014.

It's likely that the predominance of North America is due to the more stringent data breach disclosure laws in the United State compared with other countries.

Europe was next highest, well behind North America with 209 breaches (12.5%). These attacks involved 60.4 million records (9%). The Asia-Pacific region saw 131 breaches, accounting for 8% of the total and encompassing 88.1 million records (12%).

Other regions as in prior years experienced a negligible number of attacks. Even though the Middle East had just 17 breaches (1%), the number of records involved was quite high at 66.5 million (9%).

SOUTH AMERICA <1%

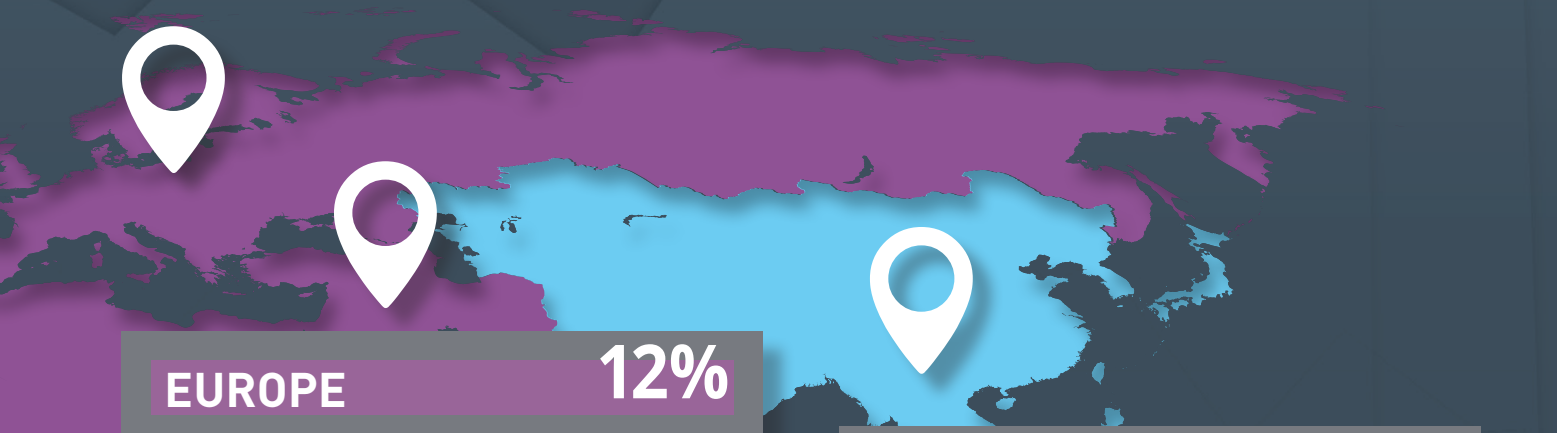
5 INCIDENTS

2	Chile
2	Brazil
1	Columbia

Africa had just seven breaches involving 820 records, and South America had five breaches involving 11,350 records. Those two regions accounted for less than one percent of the totals in both categories.

As for individual countries, the U.S. easily had the highest number of breaches, at 1,222. These accounted for nearly three quarters of all the data breaches (73%) and resulted in the compromise of 419.7 million records (59%).

2015
YEAR IN REVIEW



EUROPE 12%

209 INCIDENTS

154	United Kingdom	2	Azerbaijan
11	Germany	2	Belgium
8	Netherlands	2	Europe
7	Russia	2	Sweden
5	Italy	2	Switzerland
4	France	1	7 Countries
3	Austria		

ASIA / PACIFIC 8%

131 INCIDENTS

42	Australia	4	Hong Kong
22	New Zealand	4	Thailand
20	India	3	South Korea
12	Japan	2	5 Countries
8	China	1	2 Countries
4	Pakistan		

MIDDLE EAST / AFRICA 2%

24 INCIDENTS

5	Turkey	1	Africa
5	South Africa	1	Iran
5	United Arab Emirates	1	Seychelles
3	Saudi Arabia		

GLOBAL 1%

17 INCIDENTS

Next highest was the United Kingdom, with 154 breaches and 20.7 million records; Canada, with 59 breaches and 40.6 million records; and Australia, with 42 breaches and 105.610 records. Other countries had a relatively small number of breaches but a large number of records compromised.

For example, India had only 20 breaches but these resulted in 32.1 million records being exposed. And South Korea saw just three breaches, but 43 million records were compromised.

WHAT DOES THIS MEAN FOR DATA SECURITY

Although 2015 might not have been as bad a year in terms of high-profile data breaches as the previous year, it had its share of bad news for corporate security programs. It also showed a continuing failure among many organizations to prevent data breaches and actually protect their information assets.

For example, even though encryption technology is widely known as a means of protecting data from exposure, only 60 of the data breach incidents in 2015, (less than 4% of the total), involved data that was encrypted in part or in full.

The Breach Level Index, and the sheer number of breaches and volume of records involved in the attacks shows once again that breach prevention alone has failed many organizations.

Data breaches continue to be a large and growing threat for organizations in a variety of industries. Many are likely clinging to conventional ways of looking at cyber security, rather than taking a newer approach that will enable them to stay ahead of the attackers and more effectively protect valuable assets such as customer data, intellectual property and other resources.

The security strategy of today should include a **change of mindset**, and the implementation of solutions that **control access** and the **authentication of users**, provide **encryption** of all sensitive data, and **securely manage and store** all encryption keys.

The high-profile hacks of 2014 certainly raised awareness—at the highest levels of organizations—about the need for better security. And yet we continue to see a large number of enterprise victimized by attacks and having their data exposed.

Security, IT and business executives need to understand that having network firewalls and other network perimeter technologies are not sufficient in today's environment, in which data is distributed well beyond the enterprise boundaries. These tools must be supplemented by technologies that protect the data itself.

The security strategy of today should include a change of mindset, and the implementation of solutions that control access and the authentication of users, provide encryption of all sensitive data, and securely manage and store all encryption keys.

By creating such a strategy, organizations can more effectively prepare themselves for data breaches, and minimize the impact.

A NEW MINDSET 2015 YEAR IN REVIEW

From Breach Prevention

It's apparent that a new approach to data security is needed if organizations are to stay ahead of the attackers and more effectively protect their intellectual property, data, customer information, employees, and their bottom lines against data breaches in the future.

Security is consuming a larger share of total IT spending, but security effectiveness against the data-breach epidemic is not improving at all. In an age where data is distributed across and beyond the enterprise, **yesterday's "good enough" approach to security is obsolete.** Hackers – whether skilled criminals or insiders – both malicious and accidental are a constant threat to data.

There is nothing wrong with network perimeter security technologies as an added layer of protection. The problem is that many enterprises today rely on them as the foundation of their information security strategies, and, unfortunately, there is really no fool-proof way to prevent a breach from occurring.

To Breach Acceptance

Breach prevention is an irrelevant strategy for keeping out cyber-criminals. In addition, every organization already has potential adversaries inside the perimeter. In today's environment, the core of any security strategy needs to shift **from "breach prevention" to "breach acceptance."** And, when one approaches security from a breach-acceptance viewpoint, the world becomes a relatively simple place where securing data, not the perimeter, is the top priority. Many organizations might be inclined to address this problem with a 'containment' strategy that limits the places where data can go and only allows a limited number of people to access it. However, this strategy of "no" – where security is based on restricting data access and movement – runs counter to everything technology enables us to do. Today's mandate is to achieve a strategy of "yes" where security is built around the understanding that the movement and sharing of data is fundamental to business success.

To Securing the Breach

It's one thing to change mindsets. It's another to implement a new approach to security across an organization. While there is no "one size fits all" prescription for achieving the "Secure Breach" reality, there are three steps that every company should take to mitigate the overall cost and adverse consequences that result from a security breach. **Encrypt all sensitive data** at rest and in motion, and securely **store and manage all of your encryption keys**. **Control access and authentication of users.** By implementing each of these three steps into your IT infrastructure, companies can effectively prepare for a breach and avoid falling victim to one.

It's not a question IF your network will be breached, the only question is WHEN.

With the velocity of business accelerating, new technologies are being deployed constantly and new and sophisticated attacks are being launched regularly, is it not inevitable that it is only a matter of time before your business is hacked. Learn more at:

SECURETHEBREACH.COM

What's Your Score?

Find Out At

BREACHLEVELINDEX.COM

Contact Us: For all office locations and contact information, visit www.gemalto.com and www.safenet-inc.com