2016

It's All About Identity Theft

First half findings from the 2016

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 2016

554,454,942

NUMBER OF BREACH INCIDENTS

974

NUMBER OF BREACHES WITH OVER 1 MILLION RECORDS AFFECTED

29

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

52%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

Identity Theft is King

Identity theft has clearly become the tactic of choice for hackers, cyber criminals and other bad actors. Whereas in previous years theft of payment and financial data dominated the headlines — think of the Home Depot and Target attacks, for example — the past six months has seen the continuation of a trend that began in 2015 in which the theft of personal identifiable information has dominated.

The first half of the year is also notable in that it could put us on track for a one billion-plus year of data records lost or stolen.

These are among just some of the key findings of the latest Breach Level Index produced **by digital security technology provider Gemalto**. The numbers in the report are sobering, and even stunning, considering how much of an emphasis organizations have been placing on information security in recent years.

Key First Half Findings

According to data collected in the **Breach Level Index (BLI),** there were 974 data breaches worldwide in the first half of 2016, up 15% from the 844 breaches during the previous six months (July to December 2015), and up sharply from the 766 data breaches in the first half of 2015.

More than 554 million data records were lost or stolen in the first half of 2016, compared with some 424 million lost or stolen during the previous six months. That represents a dramatic increase of 31%. And considering that 510 of the data breaches (52%) had an unknown or unreported number compromised records, the true number of lost or stolen records is much higher.

From a time perspective, 3,046,456 data records were stolen or lost every day during the first half; 126,936 data records were stolen or lost every hour; 2,116 were stolen or lost every minute and 35 were stolen or lost every second.

To create the Breach Level Index, Gemalto, a leading global provider of digital security solutions, gathers extensive information about data breaches worldwide, using sources such as Internet searches, news articles and analyses and other resources. The data gathered is then aggregated into the Index, a database that Gemalto continually maintains. The data is analyzed in terms of the number of breaches that occur; the number of data records lost; and data breaches by industry, type of breach, source and by country or region.

DATA BREACHES

The increased targeting of individuals' identities and their personal information such as the data breaches involving Government and Healthcare organizations 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 2016 might not have had as many headline-grabbing data breaches as of yet, it certainly has seen 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 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.

The increased 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 4.8 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 so far in 2016, 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 2016 FIRST HALF REVIEW

Fling.com
Records: **40,000,000**
Type: **Identity Theft**
Score: **9.8**

The adult dating Web site was hit with an identity theft breach by a malicious outsider that resulted in the exposure of 40 million records. The attack had a BLI score of 9.8. Tens of millions of credentials stolen from the site were put up for sale on the dark web, according to International Business Times. The information reportedly included email addresses, plain text passwords, usernames, IP addresses and date of birth records.

17 Media
Records: **30,000,000**
Type: **Identity Theft**
Score: **9.7**

The software company's photo sharing and video streaming app 17 was hacked, resulting in the theft of 30 million records. The identify theft attack was committed by a malicious outsider and received a BLI score of 9.7. According to Motherboard, the hacker advertised email addresses, passwords, phone numbers, and other information from users.

Philippines' Commission on Elections
Records: **55,000,000**
Type: **Identity Theft**
Score: **9.6**

The government agency suffered an identity theft attack from a malicious outsider that accounted for the loss of 55 million records and drew a BLI score of 9.6. The group Anonymous Philippines hacked the commission's website a little over a month before the Philippines was to hold its 3rd automated elections, according to Rappler.

Mate1
Records: **27,000,000**
Type: **Account Access**
Score: **9.3**

The dating site was hit with an account access attack by a malicious outsider that involved 27 million records and received a BLI score of 9.3. A hacker in a dark web hacking forum claimed to have gained access to plaintext passwords from Mate1.com, which he later sold, according to The Next Web.

Mexican Voters
Records: **93,400,000**
Type: **Identity Theft**
Score: **9.3**

According to a number of published reports, millions of Mexican voters had their records exposed online, following an identity theft attack that affected a total of 93.4 million records and resulted in a 9.3 BLI score. Mexican election officials probing the leak of a database containing voter registration records indicated one of the main political parties in Mexico might have played a part, according to International Business Times.

VerticalScope
Records: **45,000,000**
Type: **Account Access**
Score: **9.3**

The company, which specializes in the acquisition and development of web sites and online communities for various vertical markets, experienced an account access attack by a malicious outsider that exposed 45 million records. The incident scored a BLI of 9.3. VerticalScope said it became aware that data stolen from the company was being made available online. Community member user names, email addresses, hashed passwords, and other information was involved.

U.S. Healthcare Insurer's database
Records: **9,300,000**
Type: **Identity Theft**
Score: **9.2**

An unnamed healthcare insurer was hit with an identity theft attack by a malicious outsider that resulted in the loss of 9.3 million records. It earned a BLI score of 9.2.

LEADING SOURCES OF DATA BREACHES

Who's responsible for attacks?

As in previous periods, **malicious outsiders** were the biggest source of data breaches in the first half of 2016. They were the cause of 668 breaches, or 69% of the total. That compares with 474 attacks during the previous six months, a rise of 41%.

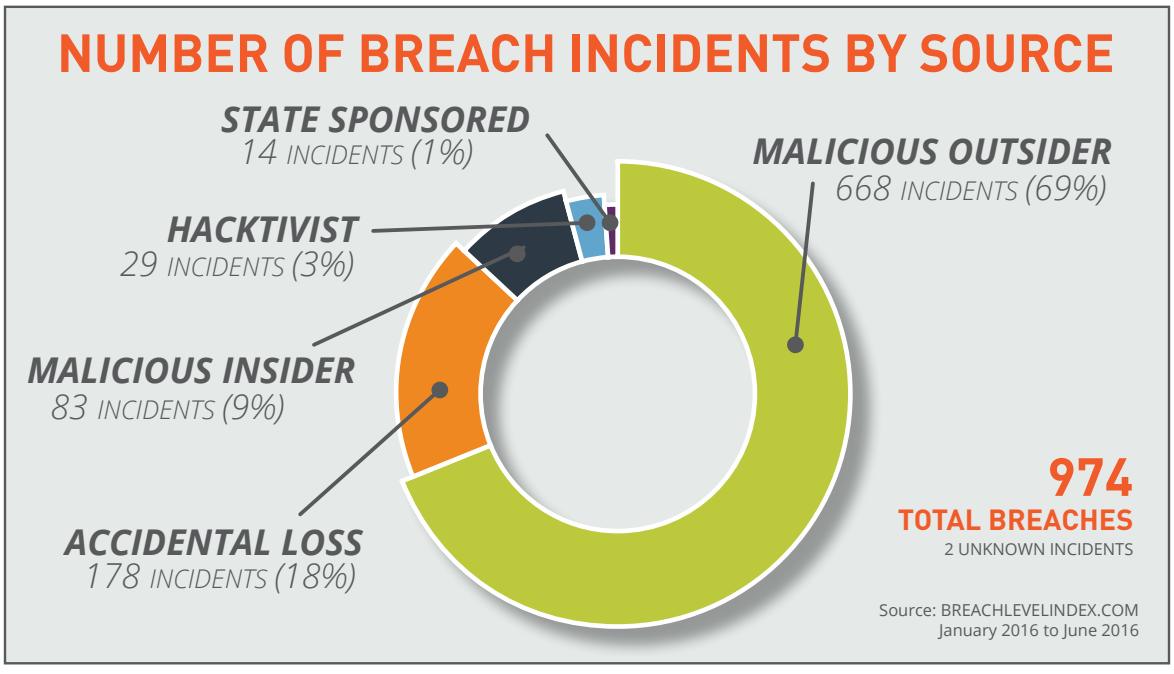
The share of attacks attributed to outsiders has climbed steadily since the first half of 2013, when it was 52%. The breaches by malicious outsiders resulted in theft or loss of some 261 million data records, or 47% of the total. That's up 23% from 96.5 million in the previous six months.

Next on the list of most common sources was **accidental loss**, which accounted for 178 data breaches (18% of the total). This was a 14% decline from the 208 breaches during the previous six months. Accidental loss involved 257 million data records (46% of the total), up from 231 million in the previous six months.

Malicious insiders were the next most common source of breaches, accounting for 83 (8.5%). That's down from 126 during the previous six months and accounted for 13.5 million data records. The records impacted was a 79% drop from the 62.8 million in the earlier period.

Hacktivists were responsible for 29 data breaches (3%), vs. 18 during the previous six months. That was an increase of 61%, and involved 11.4 million records, a significant drop from the previous 30 million.

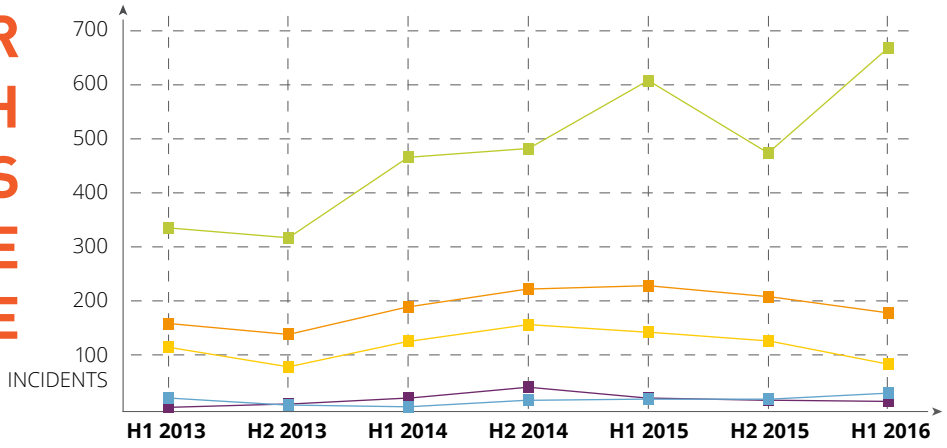
Finally, **state-sponsored** attacks accounted for 14 of the data breaches (1.4%), down from 16 over the previous six months. These attacks led to the loss or theft of 10 million data records, up from 4 million in the prior six months.



DATA BREACHES BY SOURCE OVER TIME

2016
FIRST HALF REVIEW

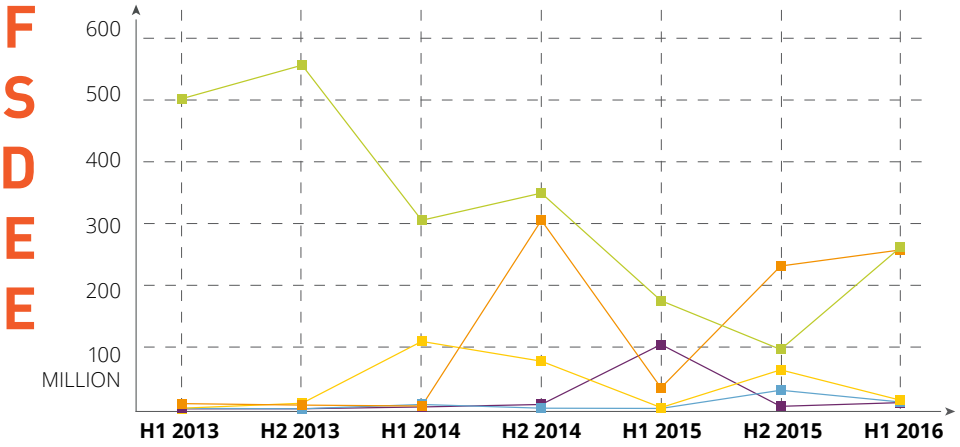
NUMBER OF BREACH INCIDENTS BY SOURCE OVER TIME



SOURCE	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016
Malicious Outsider	335	317	466	482	608	474	668
Accidental Loss	158	138	189	222	228	208	178
Malicious Insider	114	78	125	156	142	126	83
Hacktivist	20	7	4	16	18	18	29
State Sponsored	3	9	20	40	20	16	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	H1 2016
Malicious Outsider	502,693,717	556,036,710	305,036,225	349,453,283	175,502,519	96,539,842	261,378,321
Accidental Loss	8,482,892	6,140,675	4,522,782	305,299,999	33,976,903	231,231,444	257,189,614
Malicious Insider	1,150,086	9,220,723	108,570,712	76,967,930	1,946,293	62,785,175	13,454,438
Hacktivist	777,216	98,730	7,000,096	1,182,007	561,918	30,011,904	11,427,733
State Sponsored	38	165,015	3,016,499	6,912,064	104,009,225	4,067,411	10,054,836

Source: BREACHLEVELINDEX.COM

TYPES OF DATA COMPROMISED

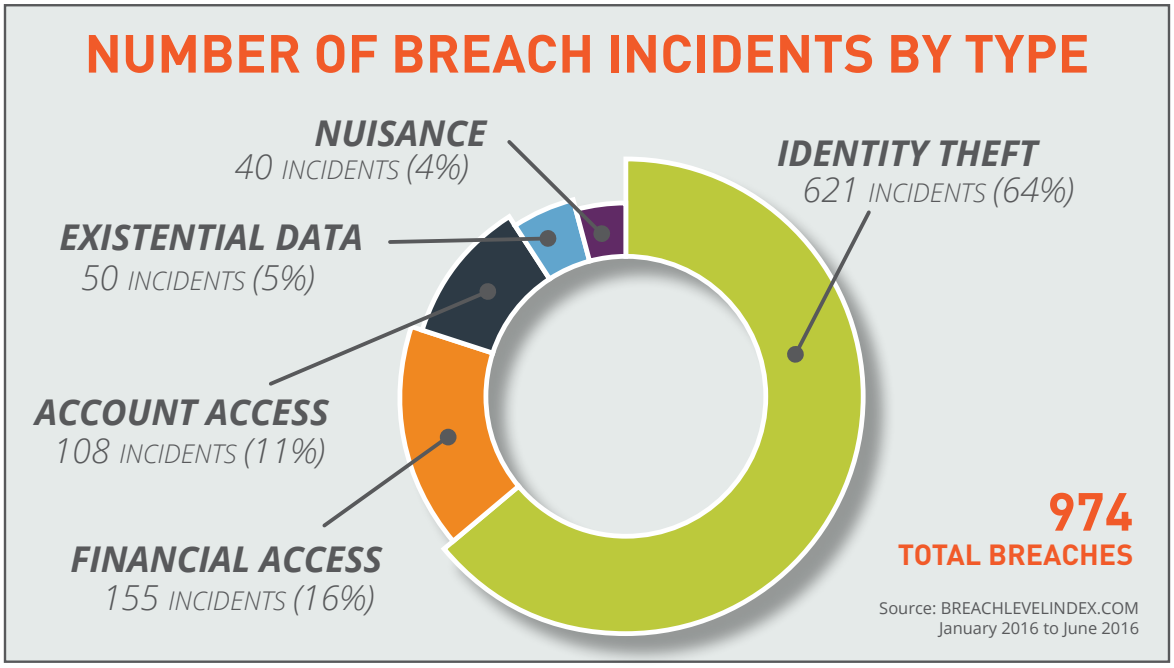
What data is targeted?

In terms of the types of data breaches that were reported in the first half of 2016, identity theft was clearly dominant. **Identity theft** attacks accounted for 621 or nearly two thirds (64%) of all the data breaches. That compares with 449 identity theft attacks (53%) during the previous six months. That's an alarming 38% increase from period to period. Identify theft has now been the leading type of data breach at least since the first half of 2013. These types of attacks involved the loss or theft of more than 294 million data records (53% of the total for the first half).

The next most common type of attack was **financial access**, the cause of 155 breaches in the first half. They accounted for 16% of the total, down from 189 during the previous six months. These attacks led to the loss or theft of 1.4 million records, compared with 2.9 million in the previous six months (a 54% decline).

Other types of attacks included **account access**, which were responsible for 108 of the data breaches (11.1%). This compares with 97 such attacks during the previous six months, a rise of 11%. Account access attacks involved 90 million data records. Much lower on the scale of attacks were **nuisance attacks** (40), which expose just user name and affiliation, and **existential data** (50). While nuisance attacks were fairly negligible in terms of the share of attacks, they did result in the loss or theft of an astounding 168 million data records (which accounted for 30% of the total). That compares with records of 268,000 in the previous six months, for an increased of 62,620%.

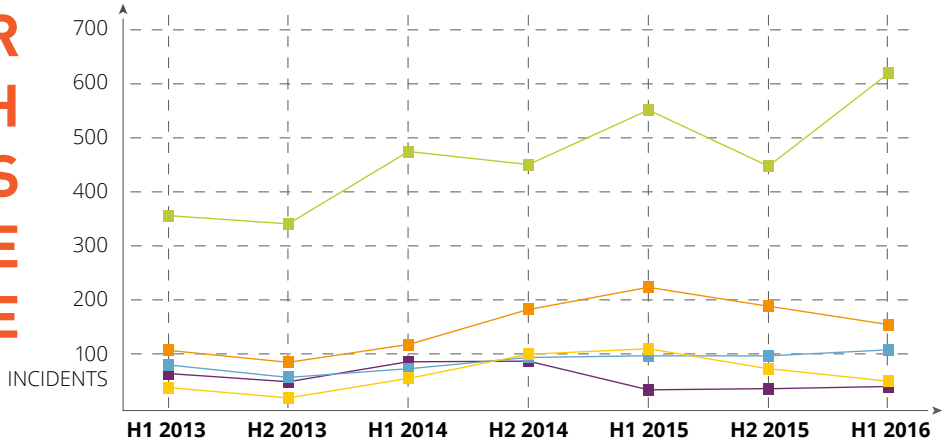
Existential data attacks caused the loss or theft of 412,000 data records, compared with 17 million in the previous six months, a decline of 98%.



DATA BREACHES BY TYPE OVER TIME

2016
FIRST HALF REVIEW

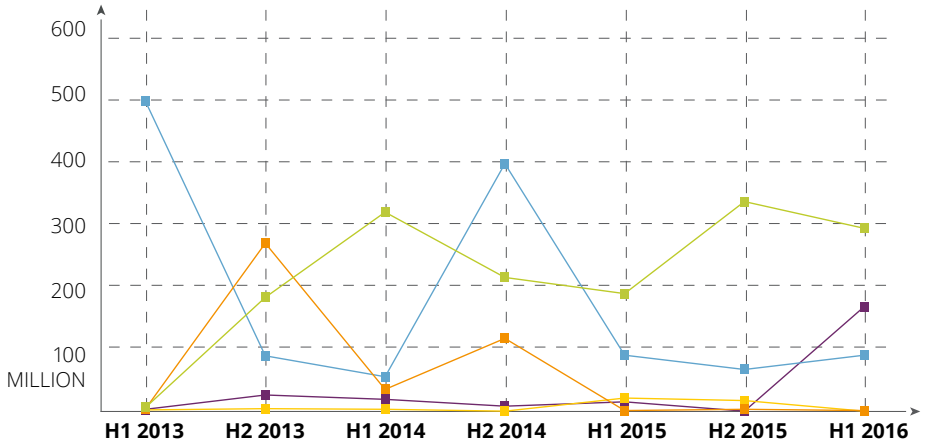
NUMBER OF BREACH INCIDENTS BY TYPE OVER TIME



TYPE OF BREACH	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016
Identity Theft	357	342	476	452	553	449	621
Financial Access	107	85	118	183	224	189	155
Existential Data	38	19	55	100	110	73	50
Account Access	80	57	73	94	97	97	108
Nuisance	64	49	86	87	34	36	40

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	H1 2016
Identity Theft	6,131,835	182,683,457	319,836,299	215,270,491	188,899,186	337,732,408	294,011,194
Financial Access	4,088,747	270,371,346	34,905,015	117,209,447	1,161,098	2,943,207	1,360,008
Existential Data	2,060,093	3,529,008	2,955,843	383,174	21,224,889	17,000,389	411,938
Account Access	498,231,533	88,923,007	50,910,557	398,530,886	89,679,608	66,691,718	90,420,937
Nuisance	2,664,521	26,159,780	19,539,907	8,421,285	15,032,468	268,254	168,250,865

Source: BREACHLEVELINDEX.COM

COMPARING THE INDUSTRIES

The **healthcare** industry has been a big target of attackers in recent years and that did not change in the first half of 2016. Healthcare led all industries with **263** data breaches, which accounted for more than one quarter (27%) of the total. This was up 25% from the 211 breaches during the previous six month period. The attacks against these organizations involved 30 million data records, or 5.4% of the total.

Next highest in the number of breaches was in **government**, which had 137 data breaches (14%) during the first half, compared with 135 during the previous six months.

Attacks against these government organizations involved over **318 million** data records more than half of all the records (57%).

Financial services was next with 118 data breaches (12%), which is close to the 123 breaches committed during the previous six months. Some 12 million data records were lost or stolen during the attacks.

The retail and education sectors each had 102 data breaches (11%) in the first half. For **retail**, that compares with 108 during the previous six months, and encompassed 16 million data records (2.9%). In the United States, there was a small spike in breaches of the point-of-sale systems at several hotel chains and retailers - most likely due to the fact that the companies had not implemented EMV and end-to-end encryption.

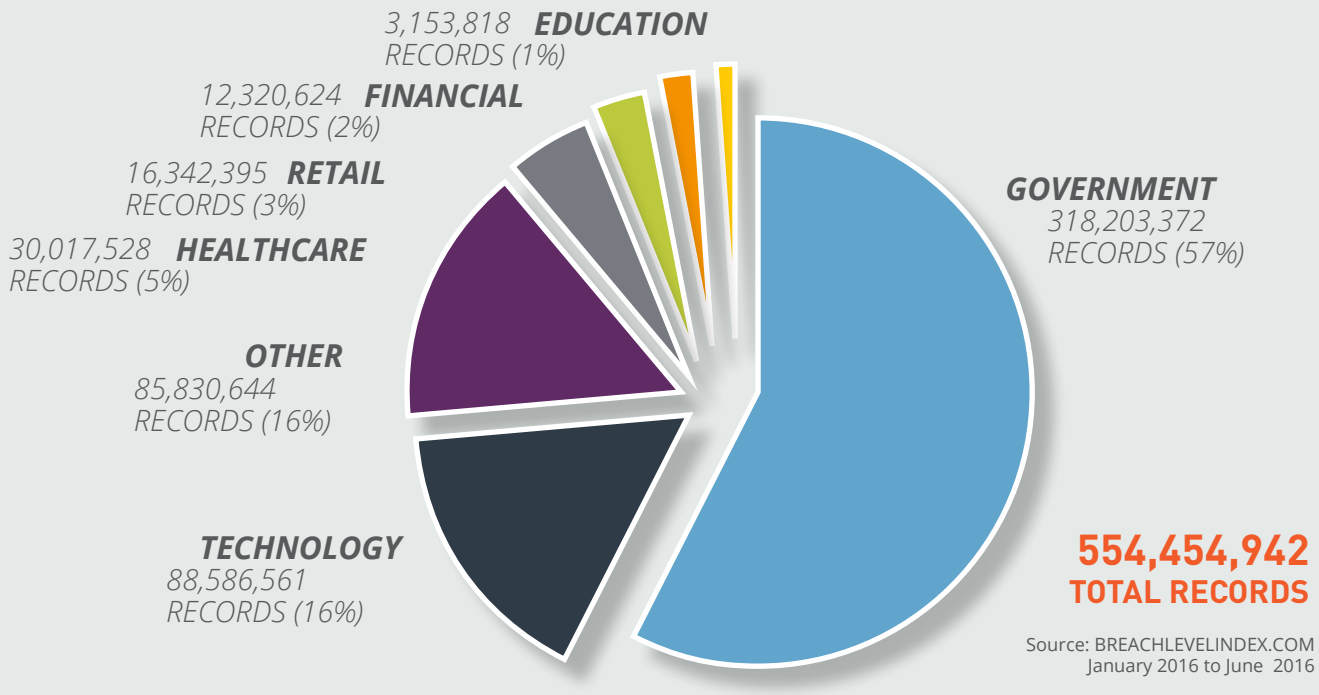
In **education**, the number of breaches was 102 (10%), compared with 63 during the previous six months, an increase of 62%. These breaches involved 3 million data records, or less than 1%.

The **technology** industry experienced 90 data breaches (9%), compared with 62 during the previous six months, a 45% increase. These companies had 88.6 million in data records lost or stolen, a 107% increase.

All other types of organizations accounted for 162 data breaches in the first half (16.4%), compared with 142 in the earlier period. The attacked involved 85.8 million data records.

COMPARING THE INDUSTRIES 2016 FIRST HALF REVIEW

NUMBER OF RECORDS BREACHED BY INDUSTRY IN FIRST HALF OF 2016



Source: BREACHLEVELINDEX.COM
January 2016 to June 2016

NUMBER OF BREACH INCIDENTS BY INDUSTRY OVER TIME

INDUSTRY	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016
Healthcare	172	168	237	208	233	211	263
Financial Services	78	86	85	126	153	123	118
Government	127	64	109	180	161	135	137
Retail	56	41	81	113	130	108	102
Education	7	27	86	87	102	63	102
Technology	55	55	72	66	58	62	90
Other Industries	151	111	138	136	181	142	162

Source: BREACHLEVELINDEX.COM

THE GEOGRAPHICAL VIEW

NORTH AMERICA 79%

772 INCIDENTS

728	United States	2	Mexico
40	Canada	2	Panama

Once again, **North America** (United States, Canada, Mexico, Central America) was easily the leading region in the number of data breaches, with 772 in the first half. That accounted for a large majority of all the breaches (79%), and compared with 628 breaches in the region during the previous six months (up 23%). The data breaches in North America involved 389.2 million data records, or 70% of the total.

SOUTH AMERICA <1%

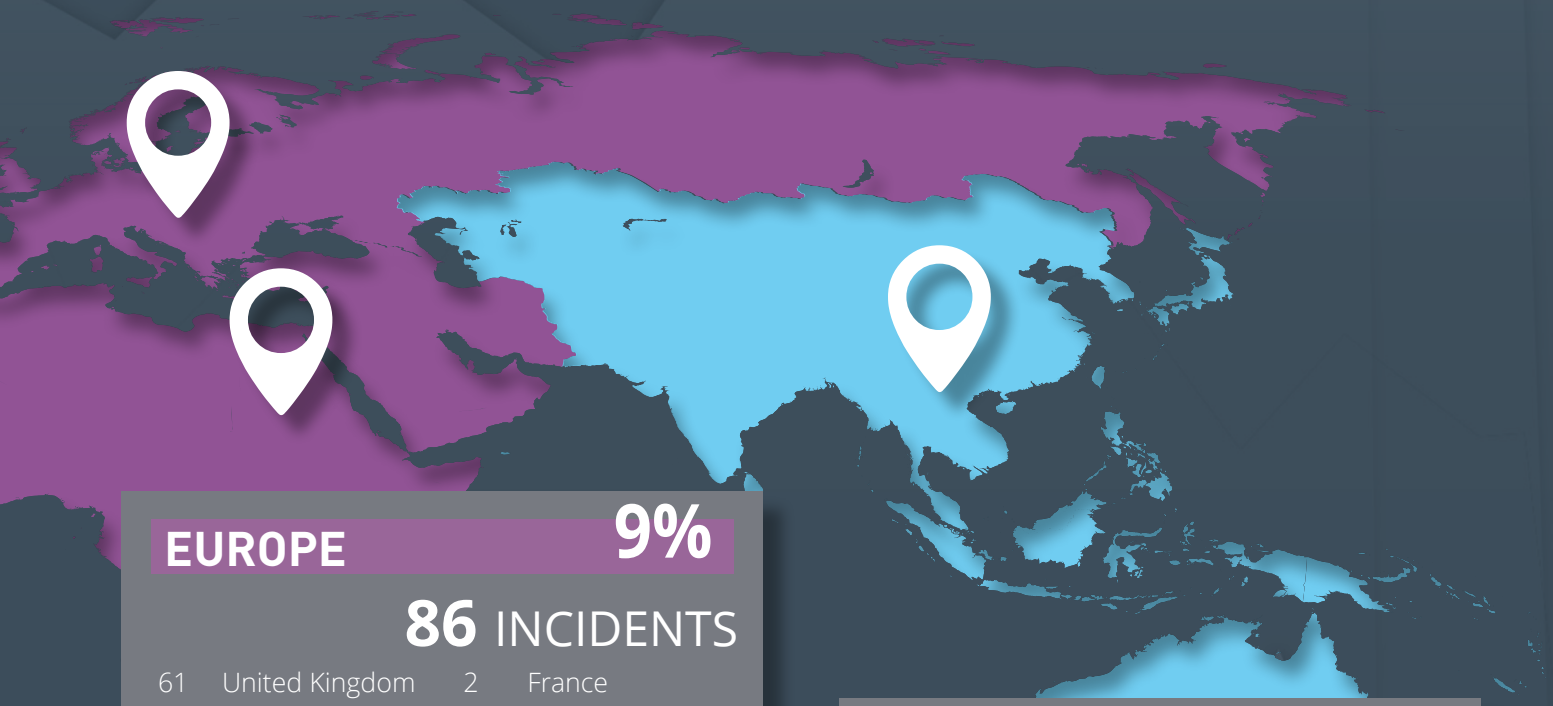
4 INCIDENTS

3	Columbia
1	Chile

The next highest region in number of breaches was **Europe**, with 86 (9% of the total). That compares with 118 breaches during the previous six months, a 27% decline, and accounted for 46.7 million data records (up 207%).

Next was **Asia Pacific**, with 76 data breaches in the first half (8%), vs. 72 during the previous six months. Breaches in the region involved 107.1 million data records (19.3% of the total). Other regions, including **Africa** (12 data breaches), the **Middle East** (nine) and **South America** (four), accounted for small shares of the total.

2016
FIRST HALF REVIEW



EUROPE 9%

86 INCIDENTS

61	United Kingdom	2	France
4	Russia	2	Netherlands
3	Germany	1	Czech Republic
3	Spain	1	Italy
2	Austria	1	Slovakia

ASIA / PACIFIC 8%

76 INCIDENTS

22	Australia		
13	India	4	China
7	Japan	3	Taiwan
7	New Zealand	2	Phillippines
5	Hong Kong	1	Cambodia
5	South Korea	1	Singapore

MIDDLE EAST / AFRICA 2%

21 INCIDENTS

5	Turkey		
5	South Africa	2	Middle East-based
5	Africa-based	2	Pakistan
2	Kenya	2	United Arab

GLOBAL <1%

7 INCIDENTS

WHAT DOES THIS MEAN FOR DATA SECURITY

Although 2016 hasn't been as bad a year in terms of high-profile data breaches as previous years, it has 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 33 of the data breach incidents so far in 2016, **(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 and 2015 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 2016
FIRST HALF 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.

What's Your Score?

Find Out At

BREACHLEVELINDEX.COM

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

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