2017

Poor Internal Security Practices Take a Toll

Findings from the first half of 2017

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 FIRST HALF OF 2017

1,901,866,611

NUMBER OF BREACH INCIDENTS

918

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

59.3%

PERCENTAGE OF DATA BREACHES WHERE ENCRYPTION WAS USED

4.6%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

EVERY DAY
10,507,550

EVERY HOUR
437,815

EVERY MINUTE
7,297

EVERY SECOND
122

Internal Threats Take Their Toll

If you're a voter in the U.S., a user of the department of motor vehicles department in India, a recipient of spam marketing content, or a patient in Britain, it's very likely that you had your personal data stolen within the past six months. That's because some of the biggest data breaches during the period were against organizations that serve those user groups.

And if you're looking for signs that data breaches are easing off and security executives can breathe a sigh of relief, hold your breath. The first half of 2017 had its share of major breaches, and the numbers are not encouraging when compared with previous data, according to a comprehensive analysis of security breaches conducted by Gemalto through data collected in its Breach Level Index (BLI).

During the first half of 2017 there were 918 data breaches worldwide, compared with 815 in the last six months of 2016. That represents a 13% increase. Of these, identity theft accounted for three quarters of data breaches, an increase of 49% compared to the previous six months.

The rise is far more dramatic in terms of the number of records involved. Some 1.9 billion data records were lost or stolen during the first half, compared with 721 million during the previous six months, an increase of 164%. There were 22 breaches in which more than 1 million records were compromised, stolen, or lost in the first half of 2017.

And this isn't even the whole story when it comes to records. More than 500 data breaches (or 59% of the total) had an unknown or unreported number of compromised records. Over the next few years, this will most likely begin to change as governments enact regulations to improve transparency surrounding data breaches.

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

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

Hackers and ransomware launchers are getting lots of the attention when it comes to security breaches. But what might be surprising to many is that a good number of the breaches in the first half of 2017 were caused by accidental loss or

DATA BREACHES

exposure of data. That includes the improper destruction of records and inadequate database security by organizations.

One example of an accidental loss breach occurred at IndyCar, which exposed the records, including personal information, of 200,000 racing fans when a database was improperly secured.

During the first half, major breaches hit organizations in a variety of industries, exposing the records of millions of individuals. Many of these records include personal information, such as patient data, and in some cases people have no idea if their information has been exposed.

The numbers on breaches and records stolen are sobering, and again make the case that organizations are failing to deploy adequate cyber security tools and processes that are needed to prevent these types of attacks from occurring.

According to the BLI, malicious outsiders were the leading source of data breaches in the first half of 2017, and accidental loss was the biggest source of lost or stolen records. Identity theft was once again the most common type of breach. In terms of geography, North America easily had the largest numbers of disclosed breaches during the first half of the year.

Following are some of the most noteworthy data breaches during the first half of 2017, including the number of compromised records, the type of breach committed, and the BLI risk assessment score. The score is calculated based on factors such as the number of records breached, the source of the breach, and how the stolen information was used by cyber criminals.

A 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 objective of the scoring system in the BLI is to show that not all data breaches have the same impact on organizations or carry the same amount of risk.

In the first half of 2017, there were several breaches with a risk score of 9.0 or above. Here's a summary of some of the top data breaches of the first half:

> While many organizations are focused on detecting and stopping outside threats, the internal threats — malicious insiders, accidental loss, and other negligence — can be a forgotten risk.

TOP NOTABLE BREACHES 2017

FIRST HALF REVIEW

Motor Vehicles Department in Kerala

RECORDS: **200,000,000**

TYPE: **Nuisance**

SCORE: **9.9**

The department suffered a data breach by a malicious outsider that led to the theft of 200 million records and rated a BLI score of 9.9, making it the highest rated breach during the first half. The database maintained by the motor vehicles department was compromised during the attack, and as a result vehicle registration details were exposed, according to the DataBreaches.net.

River City Media

RECORDS: **1,340,000,000**

TYPE: **Nuisance**

SCORE: **9.8**

The data breach against the huge email marketing organization was a nuisance breach that resulted in the theft of a staggering 1.34 billion records. This generated a BLI score of 9.8. River City Media failed to safeguard backups of its database of billion email accounts, resulting in all that user information being available for anyone to see, according to an article in Fortune.

Deep Root Analytics / Republican National Committee (RNC)

RECORDS: **198,000,000**

TYPE: **Identity Theft**

SCORE: **9.6**

Deep Root Analytics, a media firm contracted by the RNC, experienced a data breach involving 198 million records. The breach was an identity theft attack that resulted in the accidental loss of data, and rated a BLI score of 9.6. According to Fortune, the breach exposed the personal data of U.S. voters, with more than a terabyte of data stored on a publicly accessible server affected.

Zomato

RECORDS: **17,000,000**

TYPE: **Account Access**

SCORE: **9.1**

The restaurant app experienced an account access breach by a malicious outsider that exposed 17 million records, for a BLI score of 9.1. According to Engadget. The attacker infiltrated Zomato's system and got away with 17 million users' IDs, usernames, names, email addresses and hashed passwords. The service says no payment information was stolen, since credit card details are stored separately.

The National Health Service (NHS)

RECORDS: **26,000,000**

TYPE: **Identity Theft**

SCORE: **9.0**

Britain's national health services organization experienced an accidental loss breach that involved 26 million records and earned a BLI score of 9.0. The breach exposed the medical records of patients held by 2,700 practices, according to The Telegraph. Millions of patients had no idea if their records had been compromised, and the attack meant that receptionists, clerical staff, healthcare assistants and medics working in pharmacies, hospitals, and other locations could look up sensitive information about individuals, the article said.

LEADING SOURCES OF DATA BREACHES

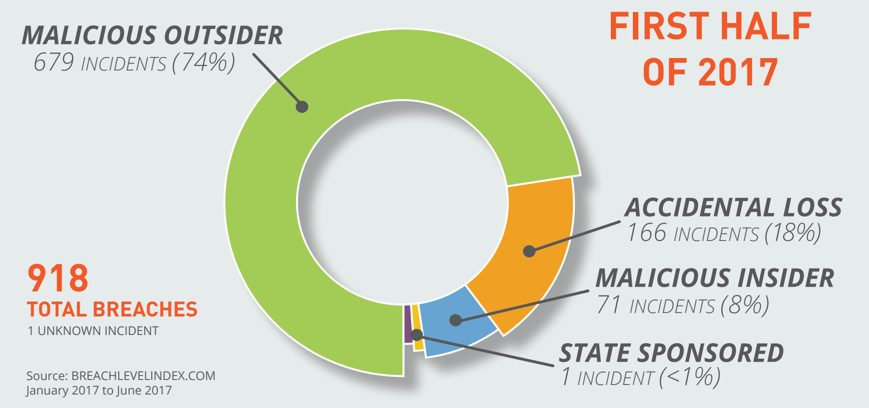
Who's Behind the Breaches?

As always, the data breaches in the first six months of the year came from a variety of sources. But in a major twist, the biggest source of lost records via data breaches was accidental loss and/or inadvertently leaving data exposed.

The number of breaches involving **accidental loss** totaled just 166, accounting for 18% of all breaches. But these attacks resulted in the theft of more than 1.6 billion records, which accounts for a whopping 86% of all records stolen in the first half via data breaches. Much of this anomaly can be attributed to the River City Media and National Health Service breaches previously noted. The number of breaches from accidental loss was up 7% from the previous six months. The number of records stolen, on the other hand, was up 4,787% from 33 million to 1.6 billion.

The next biggest source of stolen records in the period was **malicious outsiders**. This group was responsible for 679 data breaches, or 74% of the total. That resulted in the theft of 254 million records (13% of the total). The number of breaches was up 23% from the previous six months. The number of records impacted was actually down 63% from the previous six months, when 686 million records were stolen as a result of attacks by malicious outsiders.

NUMBER OF BREACH INCIDENTS BY SOURCE



Source: BREACHLEVELINDEX.COM
January 2017 to June 2017

For some perspective, consider that malicious outsiders were by far the leading source of data breaches in all of 2016, when they were responsible for more than two thirds of all the attacks launched and accounted for 76% of the total records in all breaches.

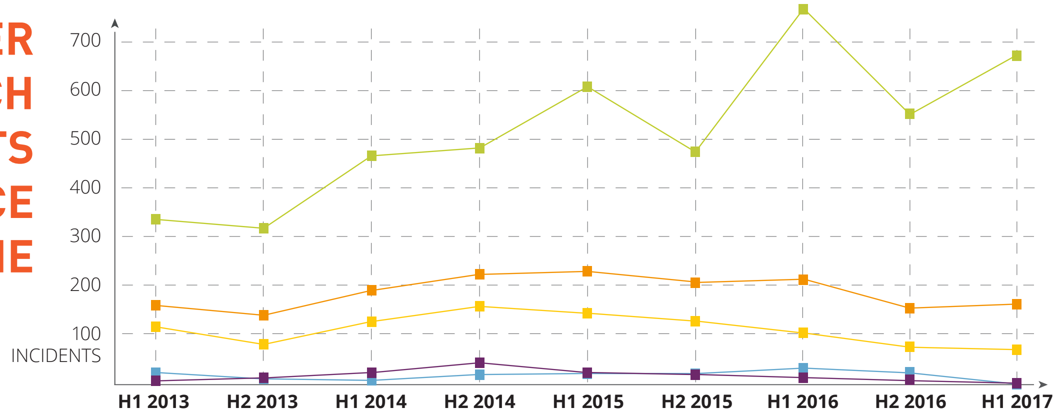
Malicious insiders were responsible for a relatively small number of attacks and records lost in the first half of 2017. The number of attacks totaled 71 (8% of the total), resulting in the loss of 20 million records (1%). The number of incidents dropped 10% from the previous six months. But the number of records involved in these attacks rose significantly (4,114%), from less than 500,000 in the previous six months.

There were no data breaches reported that were the result of an attack by **hactivists** during the first half, and only one, insignificant breach by **state sponsored** actors. This contrasts sharply with the previous six months, when there were 19 attacks by hactivists (918,000 records), and eight by state sponsored actors (442,000 records).

DATA BREACHES BY SOURCE

2017 FIRST HALF REVIEW

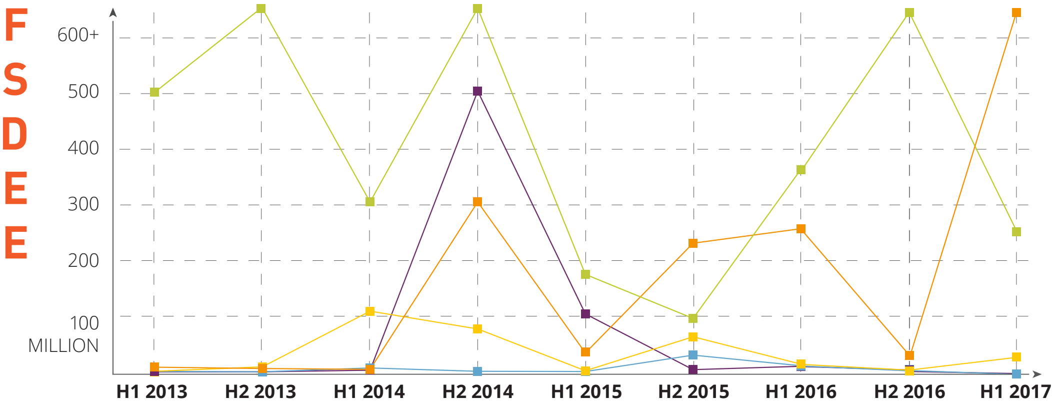
NUMBER OF BREACH INCIDENTS BY SOURCE OVER TIME



BREACH SOURCE	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017
Malicious Outsider	341	320	471	484	610	478	793	552	679
Accidental Loss	162	140	190	223	230	211	216	155	166
Malicious Insider	116	79	130	160	149	128	101	79	71
State Sponsored	3	9	20	41	20	16	13	8	1
Hacktivist	20	7	4	16	18	18	30	19	0
Unknown	16	3	4	0	2	2	2	2	1
TOTALS	658	558	819	924	1,029	853	1,155	815	918

Source: BREACHLEVELINDEX.COM

NUMBER OF RECORDS BREACHED BY SOURCE OVER TIME



BREACH SOURCE	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017
Accidental Loss	8,488,082	6,580,674	4,523,689	305,300,000	33,976,668	231,233,179	258,617,400	33,302,653	1,627,637,633
Malicious Outsider	502,709,463	1,578,575,971	305,090,925	1,569,453,283	175,502,519	99,259,842	370,439,884	686,490,243	254,017,085
Malicious Insider	1,150,087	9,221,723	108,770,712	76,968,030	2,006,460	62,785,175	13,460,128	479,618	20,211,893
Hacktivist	777,216	98,730	7,000,096	1,182,007	561,918	30,011,904	11,453,685	918,179	0
State Sponsored	38	165,015	3,016,499	506,912,064	104,009,225	4,067,411	10,355,381	442,200	0
Unknown	72,780	4,745	1,307	0	391	200	950,000	0	0
TOTALS	513,197,666	1,594,646,858	428,403,228	2,459,815,384	316,057,181	427,357,711	665,276,478	721,632,893	1,901,866,611

Source: BREACHLEVELINDEX.COM

TYPES OF DATA COMPROMISED

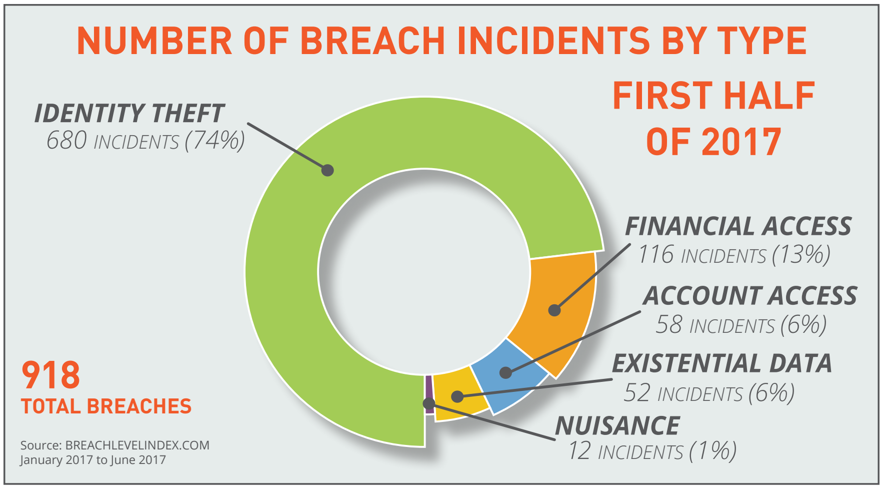
Identify Theft is Once Again on Top

As has been the case over the past several years, **identity theft** was the most common mode of attack used in data breaches in the first half of 2017. This tactic was employed for 680 data breaches, accounting for about three quarters (74%) of all the incidents during the period.

The number of breaches by identity theft jumped 49% from the previous six months, when the total was 456. The number of records stolen during these attacks saw an even bigger increase, rising 255% from 78 million to 275 million. Records involved in identity theft breaches accounted for 14.5% of the total.

> The fact that the number of identity theft breaches continues to remain high and result in many records being stolen shows that organizations are still not adequately addressing this threat.

The next most common attack mode was **financial access**. Attackers launched 116 such breaches during the first half, accounting for 13% of the total. These types of attacks decreased sharply from the previous six months (33%). The bad news is the number records stolen increased 17%, from 2.3 million to 2.6 million. Still, the records stolen only accounted for less than 1% of the total.



NUMBER OF BREACH INCIDENTS BY TYPE FIRST HALF OF 2017

Source: BREACHLEVELINDEX.COM
January 2017 to June 2017

Account access was the next most common type of data breach, with 58 incidents stemming from that mode. These accounted for just 6% of the total number of breaches, and were down 23% from the previous six months. Also down were the number of records impacted, falling 46% to 83 million from 154 million, and representing 4% of the total.

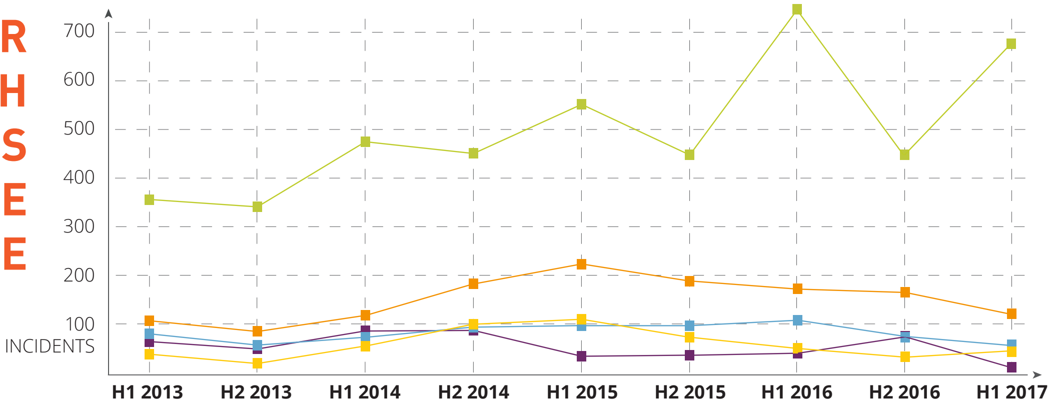
Existential data was the reason for 52 of the data breaches in the first half, accounting for 6% of the total and up 53% from the previous six months. These attacks impacted 423,000 records (less than 1% of the total), and down dramatically from 415 million in the previous six months.

Finally, **nuisance** attacks were responsible for only 12 data breaches in the first half, accounting for 1% of the total and down 84% from the previous period. But these breaches resulted in an enormous number of records being stolen: 1.54 billion, 81% of the total and up over 2,000% from 72 million in the previous six months.

DATA BREACHES BY TYPE

2017 FIRST HALF REVIEW

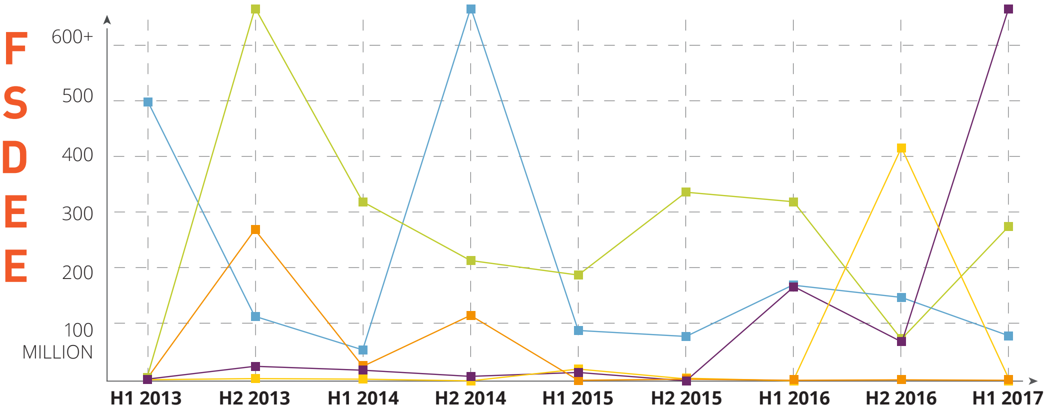
NUMBER OF BREACH INCIDENTS BY TYPE OVER TIME



TYPE OF BREACH	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017
Identity Theft	368	346	482	455	559	454	756	456	680
Financial Access	108	85	119	184	224	190	181	174	116
Account Access	80	59	74	97	100	99	111	75	58
Existential Data	38	19	57	101	112	73	63	34	52
Nuisance	64	49	87	87	34	37	44	76	12
TOTALS	658	558	819	924	1,029	853	1,155	815	918

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	H2 2016	H1 2017
Nuisance	2,664,521	26,159,780	19,539,907	8,421,285	15,032,468	268,354	168,551,929	72,249,577	1,540,006,811
Identity Theft	6,152,772	1,183,128,733	320,053,706	215,270,492	188,899,353	337,954,043	318,554,538	77,721,306	275,753,787
Account Access	498,231,533	111,457,991	50,941,357	918,530,886	89,681,373	82,191,718	175,606,078	154,442,971	83,042,615
Financial Access	4,088,747	270,371,346	34,905,015	117,209,547	1,159,098	2,943,207	2,112,970	2,260,328	2,640,115
Existential Data	2,060,093	3,529,008	2,963,243	383,174	21,284,889	4,000,389	450,963	414,958,711	423,283
TOTALS	513,197,666	1,594,646,858	428,403,228	2,459,815,384	316,057,181	427,357,711	665,276,478	721,632,893	1,901,866,611

Source: BREACHLEVELINDEX.COM

COMPARING THE INDUSTRIES

When it comes to data breaches, not all industries are equal; some have traditionally been much bigger targets than others. Here's a rundown of how the various sectors fared:

HEALTHCARE

Healthcare was the hardest hit sector in terms of the number breaches, although the number of records impacted was relatively small—but still up significantly from the previous six months. The industry experienced 228 breaches (25% of the total), which was roughly the same number of breaches in the previous six months. Some 31 million records were stolen in these attacks, accounting for 2% of the total and up 423% from just 6 million in the previous period.

FINANCIAL SERVICES

Always a popular target for cyber criminals, the **financial services** industry suffered 125 data breaches, 14% of the total and up 29% from the previous six months. Finance companies saw just 5 million records stolen as a result of these attacks, accounting for less than 1% of the total. But the number of records was up 389% from the previous six months.

EDUCATION

The **education** sector had experienced 118 breaches (13% of all breaches) that impacted a total of 32 million records (2%). The jump in breaches from the previous six months was significant at 103%. But the rise in the number of records involved was monumental at 4,957%, increasing from 641,000 records.

RETAIL

The **retail** industry, another common target for hackers and other attackers over the years, was hit by 112 breaches, or 12% of the total. That was down 10% from the previous six months, when retailers saw 125 breaches. The records involved in the data breaches was relatively low, at 4 million (less than 1% of the total). By contrast, retailers lost 16 million records in the prior six months.

GOVERNMENT

The **public sector** was victimized by 89 breaches, or 10% of the total. That was down 29% from the previous six months, when the government experienced 125 breaches. These attacks exposed a huge number of records however, totaling 404 million (21%) in the first six months, up 714% from the previous six months.

TECHNOLOGY

Technology businesses were hit with 76 breaches, accounting for 8% of the total and down 7% from the previous period. The number of records impacted dropped 72%, from 215 million to 60 million (3%).

OTHER INDUSTRIES

Data breaches in various **other industries** totaled 53, up 13% and accounting for 6% of the total. The number of records involved in these attacks was a staggering 1.34 billion (71% of the total) up from 14 million. River City Media falls under this category.

COMPARING THE INDUSTRIES

ENTERTAINMENT

Companies that provide **entertainment** services experienced just 32 data breaches in the first six months, 4% of the total and up 220% from the previous six months. Attacks targeting this industry resulted in 1.7 million lost, compromised or stolen records.

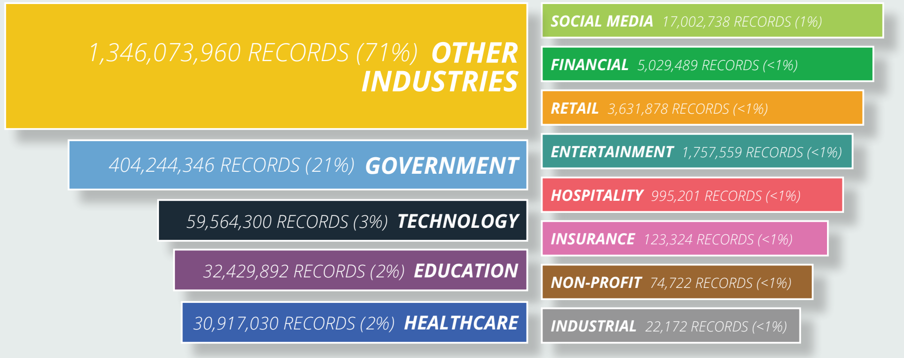
INDUSTRIAL

Companies including **industrial** manufacturers were relatively unscathed during the first six months, seeing 35 breaches (4% of the total) that resulted in the loss of only 22,000 records. Still, the number of breaches were up 218% from previous six months.

INSURANCE

Likewise, the **insurance** industry was one of the least hit by breaches. The total for the first six months was just 10 (1% of the total), resulting in the theft of 123,000 records (less than 1%).

NUMBER OF RECORDS BREACHED BY INDUSTRY IN FIRST HALF OF 2017



1,901,866,611 TOTAL RECORDS

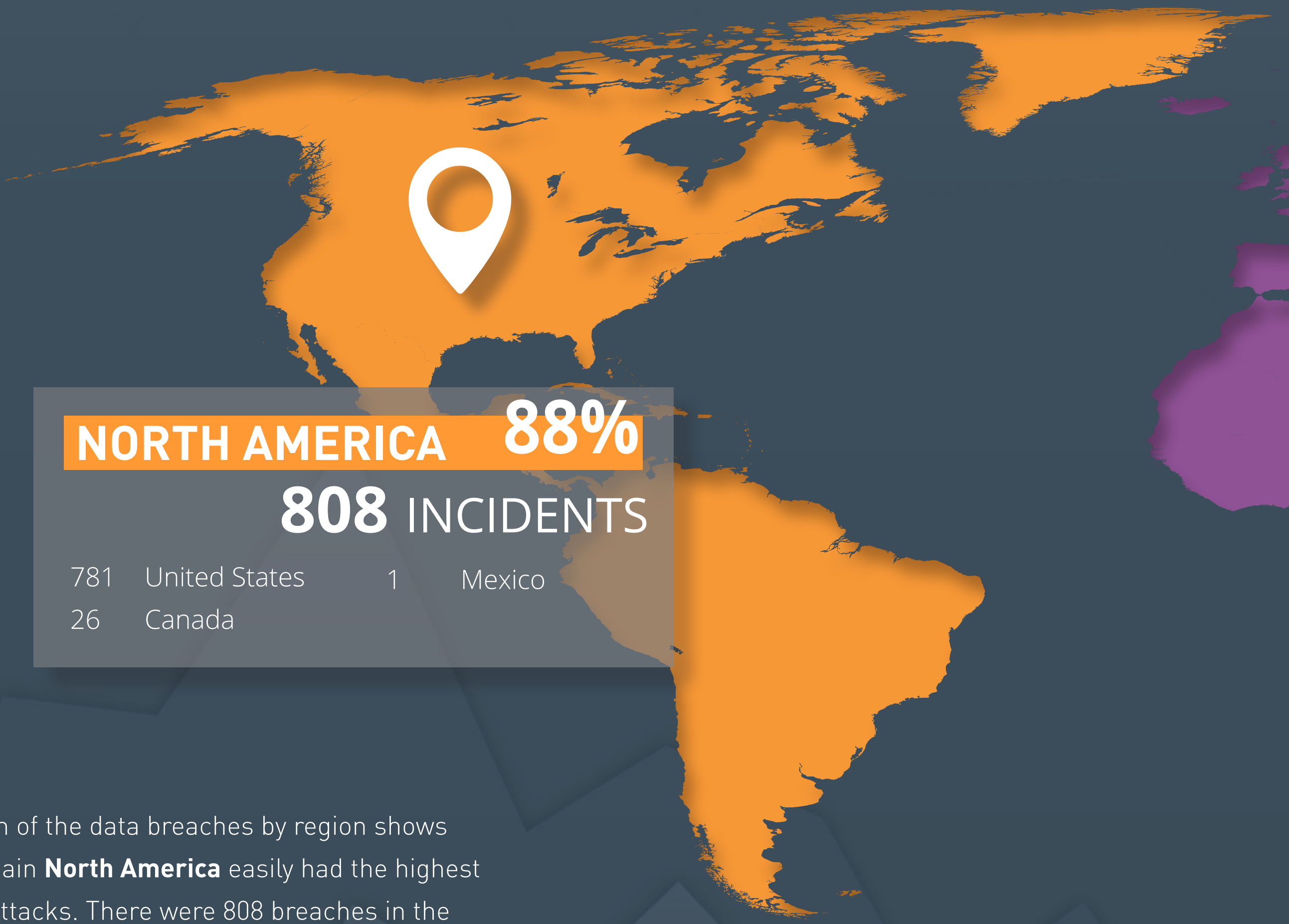
Source: BREACHLEVELINDEX.COM
January 2017 to June 2017

NUMBER OF BREACH INCIDENTS BY INDUSTRY OVER TIME

INDUSTRY	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015	H2 2015	H1 2016	H2 2016	H1 2017
Healthcare	176	170	240	209	237	214	303	229	228
Financial Services	79	86	87	126	155	123	145	97	125
Education	8	28	86	88	102	64	110	58	118
Retail	56	41	82	115	131	109	122	125	112
Government	131	65	113	180	161	137	157	125	89
Technology	55	57	73	67	60	63	119	82	76
Other Industries	152	111	138	137	177	140	130	47	53
Industrial	-	-	-	-	0	0	17	11	35
Entertainment	-	-	-	-	3	2	18	10	32
Hospitality	1	0	0	1	1	0	15	15	19
Non-Profit	-	-	-	-	0	0	10	10	15
Insurance	-	-	-	-	1	1	8	6	10
Social Media	-	-	-	1	1	0	1	0	6
TOTALS	658	558	819	924	1,209	853	1,155	815	918

Source: BREACHLEVELINDEX.COM

THE GEOGRAPHICAL VIEW



NORTH AMERICA 88%

808 INCIDENTS

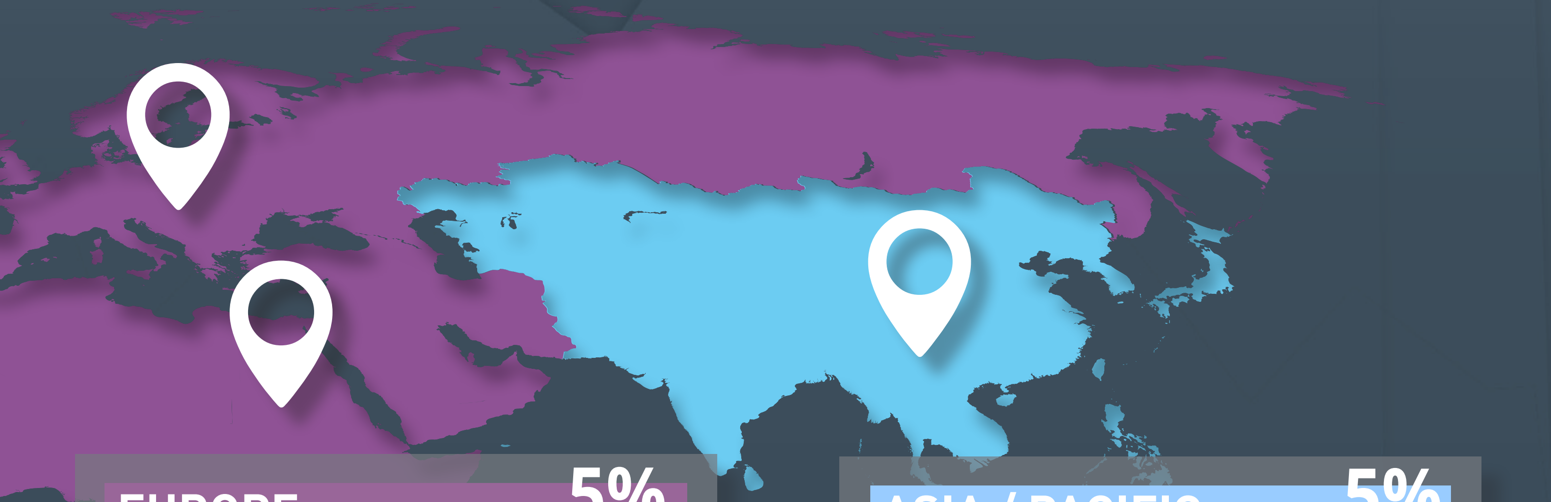
781	United States	1	Mexico
26	Canada		

A breakdown of the data breaches by region shows that once again **North America** easily had the highest number of attacks. There were 808 breaches in the U.S., Canada, Mexico, and Central America, good for 88% of all the breaches that occurred worldwide. That was up 23% from the previous six months. The number of records stolen in the North American breaches was 1.63 billion, or 86% of the total. That was up 201%.

Organizations in **Europe** were hit with 49 breaches (5% of the total), down 35% from the previous six months. These attacks resulted in the theft of 29 million records, a 79% decline from the previous six months.

The **Asia-Pacific** region experienced 47 data breaches in the first half, accounting for 5% of the total and down 27% from the previous six months.

Other regions of the world experienced much smaller numbers of breaches. **Africa** had four data breaches, down 33%, and the **Middle East** had three breaches, down 57%. Most of these regions will see a significant increase in the number of disclosed breaches and data records as governmental regulation like Europe's **General Data Protection Regulation (GDPR)** and **Australia's Privacy Act** are enforced starting in 2018.



EUROPE 5%

49 INCIDENTS

40	United Kingdom	1	Czech Republic
2	Netherlands	1	Italy
2	Malta	1	Lithuania
1	Austria	1	Norway

ASIA / PACIFIC 5%

47 INCIDENTS

15	Australia	1	Hong Kong
15	India	1	Japan
5	New Zealand	1	Malaysia
3	Singapore	1	Phillippines
2	China	1	Taiwan
2	South Korea		

MIDDLE EAST / AFRICA <1%

7 INCIDENTS

3	Middle East	1	Kenya
2	South Africa	1	Nigeria

GLOBAL <1%

7 INCIDENTS

WHAT DO ORGANIZATIONS NEED TO DO?

Based on the most recent BLI data, it's clear that organizations are still not doing enough to protect their most valuable information assets.

Consider that during the first six months of 2017, almost 11 million data records were stolen or lost every day, 437,815 every hour, 7,297 every minute, and 122 every second. Those numbers have not been getting better.

As more systems, devices and other objects become connected with the growth of the **Internet of Things (IoT)**, the threats of data breaches will likely increase.

These threats are not only coming from outside the organization. As we've seen in this most recent period, many of the breaches are the result of accidental loss or inside threats. A large portion of accidental loss are the result of **poor internal security practices or unsecure databases.** Furthermore, it's difficult to know and identify the number of vulnerable records when databases are exposed and improperly secured.

One of the main takeaways from the findings is that security needs to be comprehensive, not only including tools such as network protection and access controls, but **data encryption and multi-factor authentication** as well so in the event of a breach cyber criminals will not be able to doing anything with the stolen information.

To better protect their information assets, organizations need to take a **situational awareness approach to security** by knowing exactly where critical data resides, the threats to that data, and whether the data has been encrypted. Anything less will expose the organization—and its customers—to data breaches that can do significant harm.

> As we've seen in this most recent period, many of the breaches are the result of **accidental loss** or **inside threats**. A large portion of accidental loss are the result of **poor internal security practices** or **unsecure databases**.

Unfortunately, when it comes to encryption many organizations continue to fall short. Of the data breaches during the first six months, **only 42 (less than 5% of the total) involved data that had been encrypted in part or in full.** And under 1% of all the breached records were encrypted, dropping from over 4% encrypted during the last six months of 2016.

Security executives such as CSOs and CISOs, who have primary responsibility for protecting data and systems within their organizations, need to work with their colleagues in IT and the business lines, as well as with outside service providers if needed, to ensure that all is being done to protect these valuable resources.

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.

ENCRYPT THE DATA 01
02 STORE AND MANAGE KEYS
CONTROL USER ACCESS 03

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

Information collected from public sources. Gemalto provides this information "as-is", makes no representation or warranties regarding this information, and is not liable for any use you make of it.

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