2016

Mining for Database Gold

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

1,378,509,261

NUMBER OF BREACH INCIDENTS

1,792

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

52.2%

PERCENTAGE OF DATA BREACHES WHERE ENCRYPTION WAS USED

4.2%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

- EVERY DAY **3,776,738**
- EVERY HOUR **157,364**
- EVERY MINUTE **2,623**
- EVERY SECOND **44**

Data for Ransom

When it comes to data security breaches, 2016 was yet another year that many security executives will not remember fondly. The year saw almost 1.4 billion data records lost or stolen, up 86% from 2015, according to a comprehensive analysis of security breaches conducted by Gemalto through data collected in its Breach Level Index (BLI).

Every year seems to have its own unique trends when it comes to data security breaches, and 2016 was no exception. While significant distributed denial of service (DDoS) attacks garnered a lot of attention on the corporate security front, 2016 will also be considered the year when ransomware attacks moved into the mainstream.

A number of companies, including healthcare providers, utilities and others were willing to pay ransoms to avoid losing data or having systems shut down, showing that this type of attack is having an impact on businesses.

Perhaps more concerning for individual users, many of the attacks in 2016 got personal. The year saw a number of incidents aimed at stealing personal data on Web sites that many users might be embarrassed to admit using, such as adult content sites. In fact, there was a major increase in breaches of these sites, involving ransom requests and threats of leaking private information about their users.

By getting hold of this personal data, cyber criminals can extort victims into paying fees in order to avoid having their very private information made public. These kinds of attacks are making data breaches much more personal than other security incidents, which typically involve ransom against companies or the theft of financial data that does not expose users to public scrutiny.

Another big trend in 2016 was hackers going after large technology or social and entertainment sites to acquire account access. After gaining this access, the attackers could easily use it as an entry point.

For example, as reported in an article on the Forbes site in December 2016, hackers stole millions of dollars in bitcoin using only phone numbers. The article noted a spate of recent hackings of high-profile cryptocurrency

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

capitalists and others who have had their phone numbers hijacked and suffered financial losses.

Also notable about 2016 is that it was a year in which the scale of records lost, stolen or compromised during data breaches was much larger than in previous years. The key implication of this is that hackers are casting a wider net whenever they launch an attack against a given target.

Hackers and other attackers launched 1,792 data breaches worldwide in 2016, according to the Gemalto's BLI.

The number of breaches was actually down 4% from 1,866 the year before, but still significant and damaging when you consider that almost 1.4 billion data records were lost or stolen in 2016 compared with 740 million in 2015. That represents and increase of 86%.

> Once again cyber security efforts are not preventing attacks from being successful.

Given that in some cases the number of records involved in a breach are not disclosed, the actual number of lost and stolen in data breaches might even be a lot higher. In other instances, like Yahoo!, it can take years for companies to identify or disclose a breach. But the numbers that are available on breaches and records stolen in 2016 are eye-opening, and once again show that cyber security efforts are not preventing these attacks from being successful.

And consider that 936 out of the 1,792 breaches had an unknown amount of data records involved, because the information was not publicly available in the breach disclosure. This is noteworthy as it represents the difficulty of knowing exactly how many people's records have been affected. Breach disclosure laws only require certain things such as informing people if they have been affected.

According to the BLI, malicious outsiders such as hackers and cyber criminals were by far the leading source of data breaches in 2016. Once again, identity theft was the most common type of breach. Of the industry sectors, healthcare was easily the hardest hit with breaches. And in terms of geography, the United States and North America had by far the largest numbers of disclosed breaches during the year.

Following are some of the most notable data breaches in 2016, including the number of compromised records, type of breach, 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.

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 point of 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. Many of the top breaches were through account access and identity theft.

TOP SCORING BREACHES

2016 YEAR IN REVIEW

Adult FriendFinder

Records: **412,214,295**
Type: **Account Access**
Score: **10.0**

The Internet-based, adult-oriented social network and online dating service was hit with an account access data breach by a malicious outsider that exposed over 400 million records. The breach scored the max of 10 on the risk assessment scale. The hacked database includes customers' e-mail addresses, IP addresses last used to log-in to the site, and passwords, according to Ars Technica.

Philippines' Commission on Elections

Records: **77,736,795**
Type: **Identity Theft**
Score: **9.8**

The data breach against the commission, an identity theft attack by a malicious outsider, resulted in the theft of 77.7 million records. The BLI score was 9.8. The breach appeared to contain millions of fingerprint records, despite officials claiming the leak did not include biometrics, according to Wired.

Fling.com

Records: **40,000,000**
Type: **Identity Theft**
Score: **9.8**

The adult-orientated Web site and social network experienced an identity theft breach by a malicious outsider that exposed 40 million records, earning it a BLI score of 9.8. The passwords and sexual preferences of users were put up for sale on the dark web, according to International Business Times.

17 Media

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

The provider of an app for live streams and photos had an identity theft breach by a malicious outsider that exposed 30 million records, for a 9.7 BLI score. According to Motherboard, the data, advertised on the dark web, includes phone numbers, IP addresses and details about users' phone models.

Daily Motion

Records: **85,000,000**
Type: **Account Access**
Score: **9.5**

The video sharing platform experienced an account access breach resulting in the theft of 85 million records, for a BLI score of 9.5. News site Bleeping Computer reported that based on samples it received and analyzed the stolen information included user IDs, emails and hashed passwords.

Kerala

Records: **34,000,000**
Type: **Identity Theft**
Score: **9.4**

According to news reports, millions of people in the Kerala region of India had their data compromised. The incident has a BLI score of 9.4. 34 million Keralites were affected by the massive data leak of sensitive information such as income, name, date of birth and other personal identifiable information.

Evony Gaming Company

Records: **33,407,472**
Type: **Account Access**
Score: **9.4**

Over 33 million gamers using the website Evony Gaming Company had their account information stolen. The account access attack resulted in a BLI score of 9.4

LEADING SOURCES OF DATA BREACHES

Malicious Outsiders Strike Again—and Again

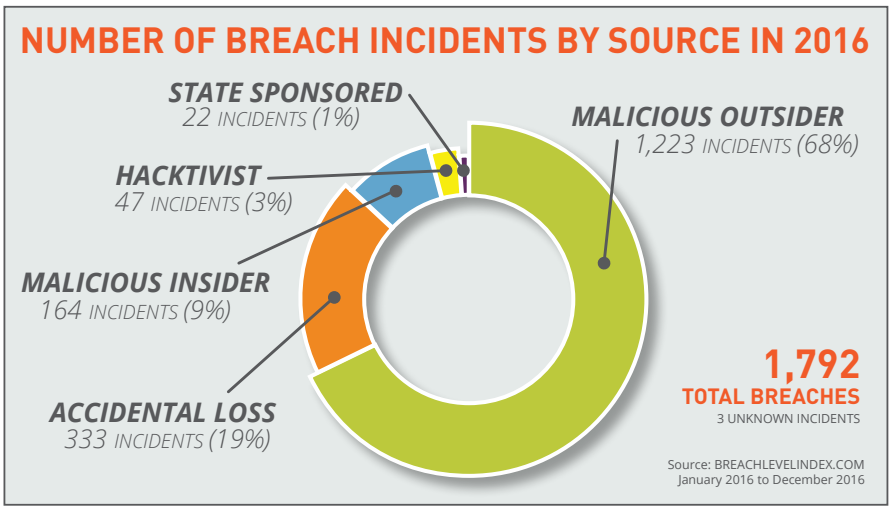
In order to be better equipped to protect corporate data against attacks, organizations need to have a clear sense of where the attacks are coming from, who's behind them and what tactics they are using to carry out the breaches.

By far, the leading source of data breaches in 2016 was **malicious outsiders**. This group was responsible for 1,223 data breaches during the year, which accounted for more than two thirds of all the attacks launched (68.2%). That compares with 1,082 breaches in 2015 (58% of the total), and represents an increase of 13%.

Breaches from these malicious outsiders involved some 1.05 billion records (76.2% of the total records in all breaches in 2016), up an astounding 286.1% from 272 million the year before. What could account for such a huge increase?

The next biggest source of data breaches in 2016 was **accidental loss**, although the number of these incidents dropped from the year before. Some 333 data breaches (18.6%) were caused by accidents, compared with 437 (23.4%) in 2015. That's down 23.8% year to year. However, the number of records involved in such breaches increased 9.4%, from 2.65 million in 2015 to 2.90 million.

Also getting a lot of attention in recent months are **state-sponsored** security attacks, so it's somewhat surprising that the number of these types of breaches was down in 2016. State-sponsored hackers launched 22 data breaches (1.2%)



For all the attention given to the threat of attacks from inside organizations, **malicious insiders** were responsible for only 164 of the data breaches in 2016 (9.2% of the total). That's down 39.5% from 271 data breaches the year before, when insider breaches accounted for 14.5% of the total. Breaches involving malicious insiders exposed 13.9 million records in 2016, or roughly 1% of the total. By comparison, these types of breaches involved 64.7 million records in 2015, or 8.7% of the total.

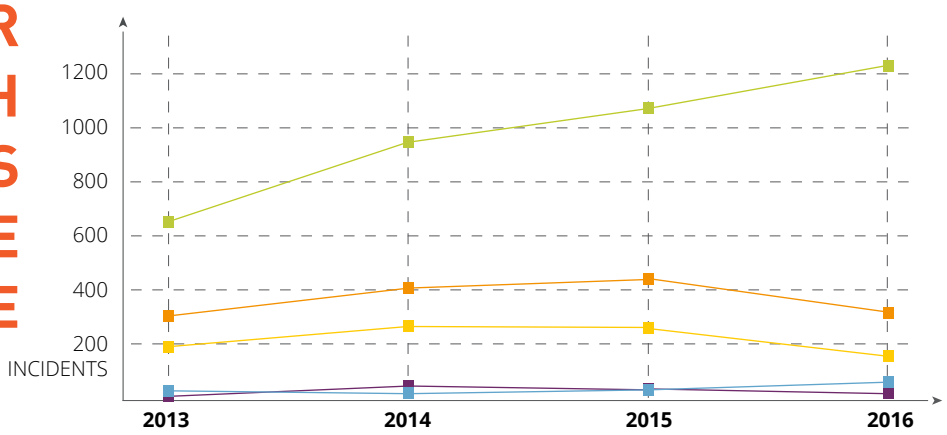
in 2016, compared with 36 breaches in 2015, for a decrease of 38.9%. Also down was the number of records affected by these attacks, from 108 million in 2015 to 10 million in 2016.

State-sponsored attackers were actually exceeded in the number of breaches by **hacktivists**, who were responsible for 47 breaches in 2016, accounting for 2.6% of the total and up 30.6% from 36 breaches in 2015. Hacktivist attacks exposed only 12.4 million records in 2016, less than 1% of the total.

DATA BREACHES BY SOURCE OVER TIME

2016 YEAR IN REVIEW

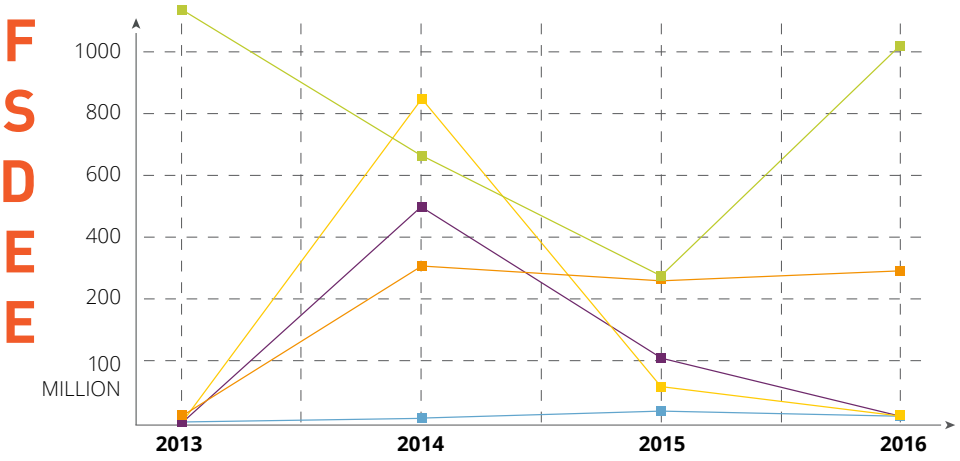
NUMBER OF BREACH INCIDENTS BY SOURCE OVER TIME



SOURCE	2013	2014	2015	2016
Malicious Outsider	659	950	1,082	1,223
Accidental Loss	300	412	437	333
Malicious Insider	194	286	271	164
Hacktivist	27	20	36	47
State Sponsored	12	61	36	22

Source: BREACHLEVELINDEX.COM

NUMBER OF RECORDS BREACHED BY SOURCE OVER TIME



SOURCE	2013	2014	2015	2016
Malicious Outsider	2,081,285,434	654,506,008	272,042,361	1,050,297,092
Accidental Loss	15,024,803	309,822,782	265,206,447	290,161,444
Malicious Insider	10,371,809	878,250,642	64,731,468	13,931,926
Hacktivist	875,946	8,182,103	30,573,822	12,371,763
State Sponsored	165,053	509,928,563	108,076,636	10,797,036

Source: BREACHLEVELINDEX.COM

TYPES OF DATA COMPROMISED

Identify Theft Tops as Leading Mode of Attack

Once again **identity theft** was the most common type of attack used in data breaches in 2016, the third straight year that has been the case. Identity theft was used for 1,050 data breaches, well over half of all the incidents and accounting for 58.6% of the total.

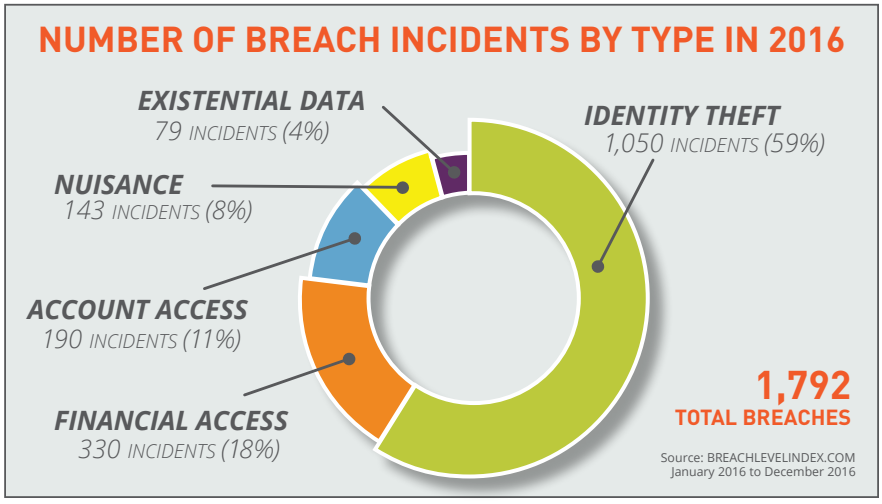
The number of breaches was up slightly from 1,004 in 2015. However, a substantial decrease was in the number of records stolen via identity theft in 2016: nearly 400 million (28.4% of the total), down 25.8% from 526.6 million in 2015. Given this trend that has developed with identify theft as the leading attack model for breaches, it's clear that companies are not doing enough to address this threat.

Criminals naturally gravitate to where the money is, so it's not surprising that the next most common form of data breach in 2016 was **financial access**. Attackers launched 330 such breaches during the year, accounting for 18.4% of the total.

It's interesting to note that these types of attacks were down by 20.1% from 413 in 2015. But the number of data records stolen increased by 32.8%, from 4.1 million to 5.4 million.

Next on the list of most common types of breaches is **account access**, which was the method for 190 breaches in 2016 (10.6%).

Nuisance attacks were responsible for 143 data breaches in 2016, accounting for 8% of the total and up dramatically (101.4%) from the 71 attacks the year before. Even more dramatic was the rise in records stolen. These attacks led to the theft of almost 241 million records (17.5% of the total) in 2016, compared with just 15.3 million in 2015.



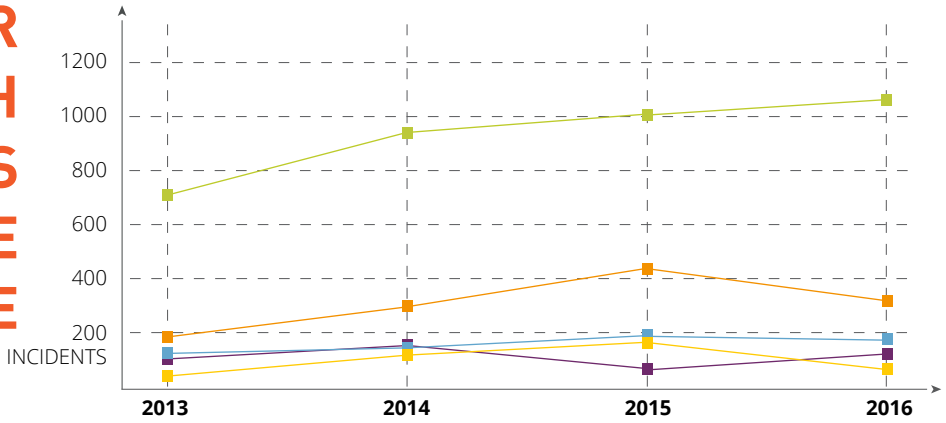
These account access breaches were down slightly from 2015's total of 196 attacks. And while the number of breaches was relatively small, they impacted an extraordinary number of records, 738 million. That represents more than half (53.6%) of all the records in data breaches in 2016, and is up 336% from 169 million in 2015.

Finally, **existential data** was the cause of 79 data breaches in 2016 (4.4%), down 56.6% from 182 data breaches in 2015. These attacks led to the loss of 3.1 million data records (less than 1%), and were down 87.5% from 2015.

DATA BREACHES BY TYPE OVER TIME

2016 YEAR IN REVIEW

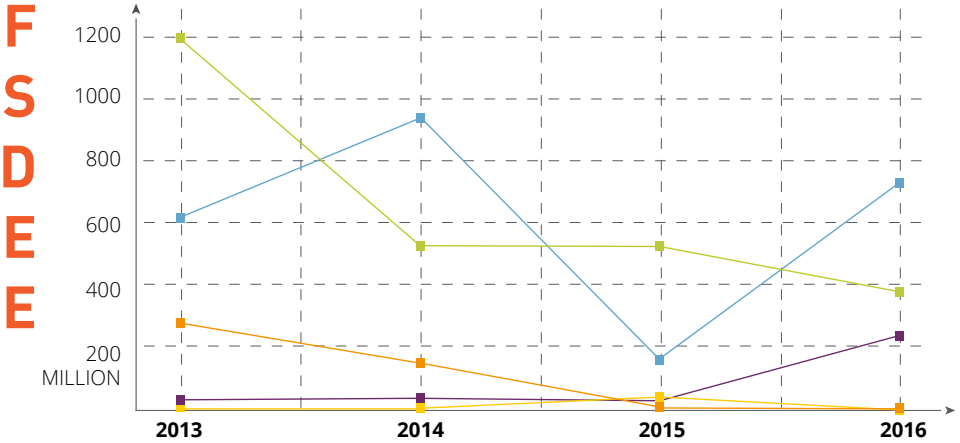
NUMBER OF BREACH INCIDENTS BY TYPE OVER TIME



TYPE OF BREACH	2013	2014	2015	2016
Identity Theft	710	935	1,004	1,050
Financial Access	192	301	413	330
Account Access	139	168	196	190
Nuisance	113	174	71	143
Existential Data	57	155	182	79

Source: BREACHLEVELINDEX.COM

NUMBER OF RECORDS BREACHED BY TYPE OVER TIME



TYPE OF BREACH	2013	2014	2015	2016
Account Access	609,689,524	949,441,443	169,371,326	738,269,220
Identity Theft	1,189,237,551	535,123,291	526,631,594	390,810,752
Nuisance	28,824,301	27,961,192	15,300,822	240,835,910
Financial Access	274,460,093	152,114,462	4,102,305	5,447,249
Existential Data	5,589,101	3,339,017	25,225,278	3,146,130

Source: BREACHLEVELINDEX.COM

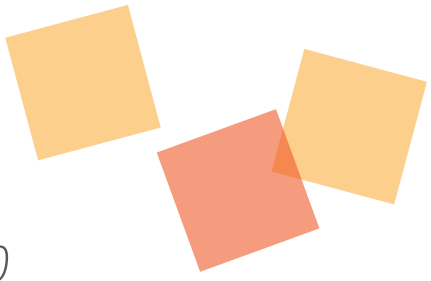
COMPARING THE INDUSTRIES

Some sectors were hit harder with data breaches than others in 2016. Here's a look at how a number of industries fared:

HEALTHCARE

The **healthcare** industry was the hardest hit during the year in terms of the number of data breaches, accounting for more than one quarter (27.5%) of all breaches. Healthcare organizations experienced 493 breaches, compared with 445 in 2015, for an increase of 10.8%.

However, despite the rise in breaches the number of records stolen dropped 75.4%, from 143.2 million in 2015 to 35.3 million in 2016. Part of this is due to the fact that in 2015 Anthem had a massive breach in which the number of records was disclosed. But in 2016 many of the healthcare breaches didn't have numbers associated with them.



GOVERNMENT

The public sector experienced the opposite of what the healthcare industry did, with breaches down from the year before and records up. Agencies and other **government** entities had 269 breaches in 2016, down 9.4% from the previous year and accounting for 15% of the total.

The number of records lost or stolen in attacks against the government totaled 391.7 million, up 27.3% from 2015 and accounting for about one quarter of all the records involved in data breaches in 2016 (28.4%).

RETAIL

The **retail** sector has taken significant steps to stop cyber attacks—particularly at the point of sale—and perhaps it's paying off. Retailers had 215 data breaches in 2016, down 10% from 239 the year before and accounting for 12% of the total. Also down was the number of records stolen—to 32.5 million from 40.1 million in 2015. That was a decrease of 18.8%

FINANCIAL SERVICES

The **financial services** sector is one of the more fascinating, and gives a good indication of how attacks are resulting in the theft of larger numbers of records. The number of breaches in the industry declined 22.5% to 214 from 276 in 2015, accounting for 11.9% of the total.

But the number of records lost or stolen in these attacks went from just 1.1 million in 2015 to 13.3 million in 2016. That represents a massive rise of 1,070%.

TECHNOLOGY

Attacks against **technology** companies, mainly businesses that offer technology services to clients, rose sharply in 2016. The number of breaches jumped 54.9% to 189, accounting for 10.5% of the total. Even more alarmingly, the number of records stolen from these companies soared 277.5% to 391.6 million, from 103.7 million in 2015. The technology sector accounted for more than one quarter of all the records stolen in 2016, 28.4%.

COMPARING THE INDUSTRIES

2016 YEAR IN REVIEW

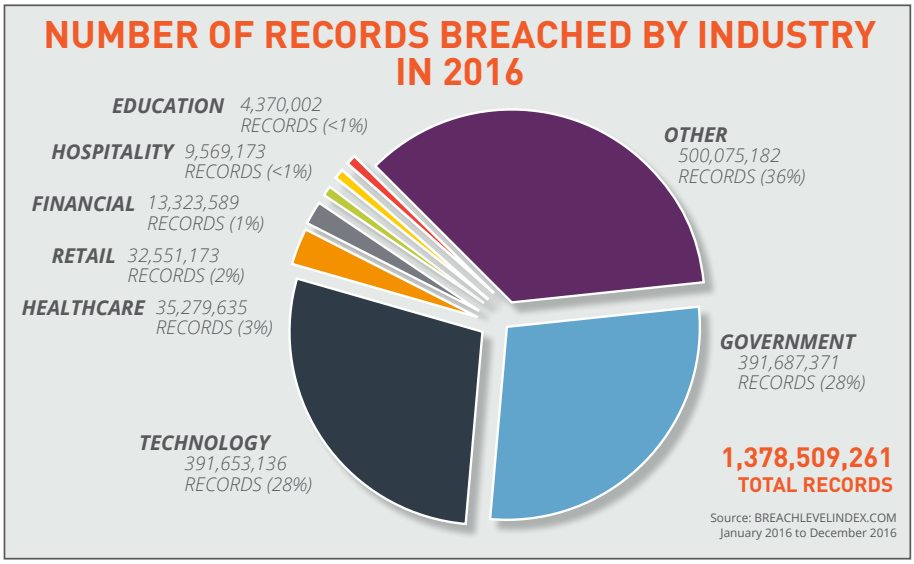
EDUCATION

The **education** sector saw improvements in both the number of data breaches and records. Breaches totaled 157, down 4.8% and accounting for 8.8% of the total. Records stolen dropped 78.1% to 4.4 million.

HOSPITALITY

The good news for the **hospitality** industry is that it was the least hardest hit of the sectors evaluated, with 26 data breaches (1.5% of the total) in 2016. The bad news is that number of breaches rose greatly from just one breach in 2015. Records lost totaled 9.6 million, up from an undisclosed amount the year before.

Breaches in industries other than those above, including social and entertainment sites, totaled 229 in 2016. That accounted for 12.8% of the total and was down 28.7% from 321 in 2015. A tremendous volume of records were involved in these attacks: 500 million, accounting for 36.3% of the total. That was up 300% from 124.8 million in 2015.



NUMBER OF BREACH INCIDENTS BY INDUSTRY OVER TIME

INDUSTRY	2013	2014	2015	2016
Healthcare	345	448	445	493
Government	194	290	297	269
Other Industries	262	275	321	229
Retail	98	195	239	215
Financial Services	165	212	276	214
Technology	112	139	122	189
Education	35	174	165	157
Hospitality	-	-	1	26

Source: BREACHLEVELINDEX.COM

THE GEOGRAPHICAL VIEW

NORTH AMERICA 80%

1,433 INCIDENTS

1,348	United States	3	Mexico
77	Canada	2	Panama
3	North America-based		

Once again **North America** dominated in the regional breakdown of data breaches, accounting for 80% of all breaches. The total number of breaches in the United States, Canada, Mexico and Central America was 1,433, up 11.3% from the year before.

Attacks in the region resulted in the theft of 1.0 billion records, or about three quarters of all breaches worldwide (73.3%). This was up 119% from 462.5 million in 2015. As in past years, 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 had the next highest number of data breaches, with 161. That accounted for 9% of the total in 2016, and down 23% from 209 breaches in 2015. The attacks in European countries resulted in the theft or loss of 183.4 million records (13.3%), up 93.5% from 94.8 million the year before.

SOUTH AMERICA <1%

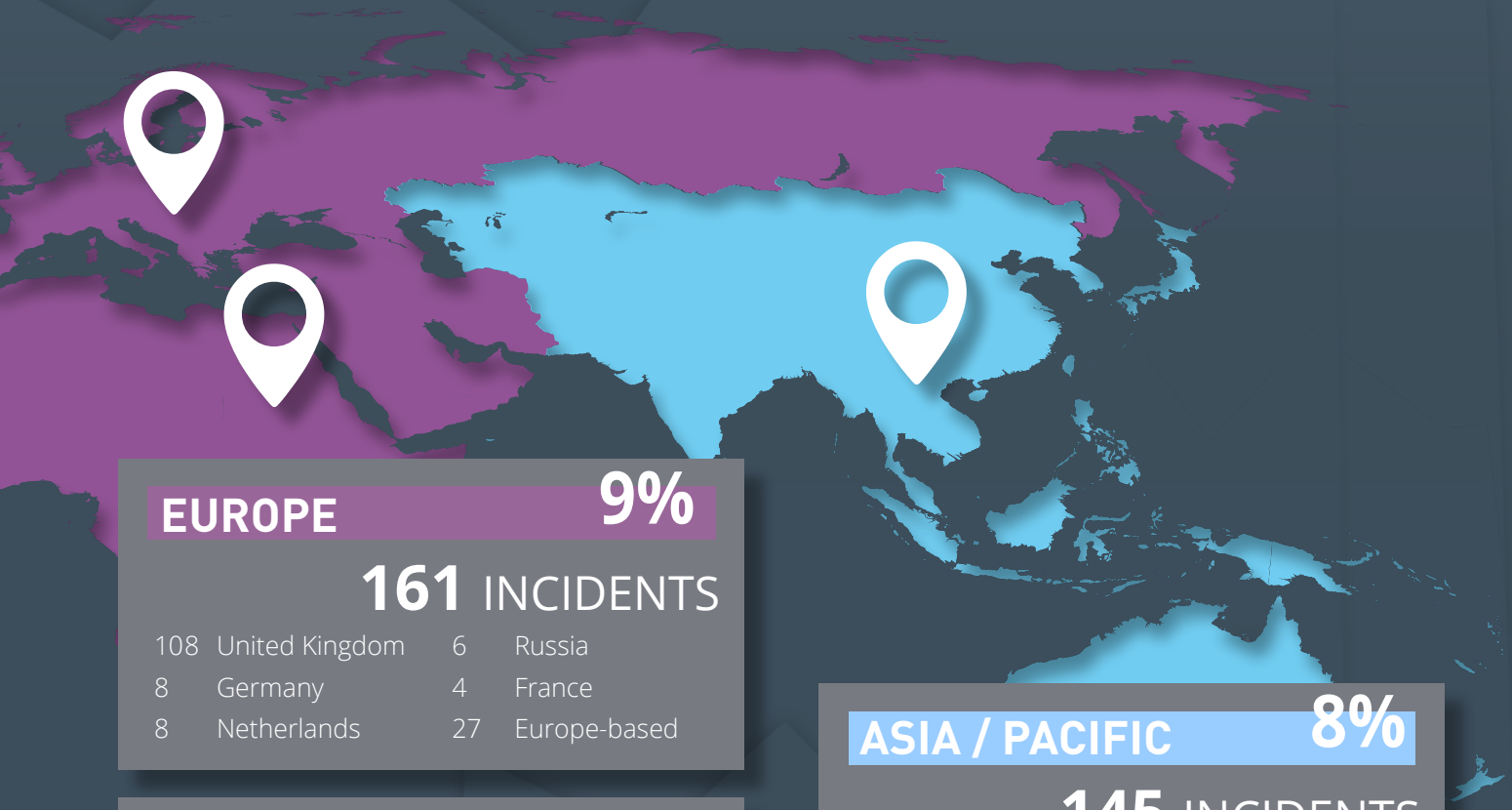
7 INCIDENTS

3	Columbia	1	Paraguay
1	Argentina	1	Venezuela
1	Chile		

The **Asia-Pacific** region experienced 145 data breaches in 2016, accounting for 8.1% of the total and up 10.7% from 2015. Some 138 million records were stolen in these attacks, drastically up from 1.3 million in 2015.

Other regions of the world experienced much smaller numbers of breaches. The **Middle East** had 21 breaches, up from 18 in 2015. They resulted in the theft of 45.2 million records, compared with 38.5 million in 2015. **Africa** had 17 data breaches compared with six in 2015; and **South America**

2016
YEAR IN REVIEW



EUROPE 9%

161 INCIDENTS

108	United Kingdom	6	Russia
8	Germany	4	France
8	Netherlands	27	Europe-based

ASIA / PACIFIC 8%

145 INCIDENTS

44	Australia	7	Hong Kong
24	India	7	South Korea
16	New Zealand	7	Taiwan
12	Japan	6	Thailand
11	China	11	APAC-based

MIDDLE EAST / AFRICA 2%

38 INCIDENTS

9	South Africa	18	Middle East-based
6	Turkey	5	Africa-based

GLOBAL <1%

8 INCIDENTS

had seven breaches compared with five the year before. Records stolen in both of these regions was relatively negligible.

The U.S. had by far the highest number of breaches of any country, 1,348 attacks that resulted in the theft of 858 million records. Next was the United Kingdom with 108 breaches (54.5 million records) and Canada, 77 breaches (46.1 million records).

WHAT DOES THE DATA SAY?

Over the past four years, the state of data breaches has changed. Two of the biggest known breaches since 2013 only came to light last year, totaling a staggering 1.5 billion records. Yahoo! announced them several years after they happened. While the scale of the breach is concerning, it is the delay in disclosing or identifying them that is most concerning.

As a new era of connected devices begins, one of the most important things organizations can do is reduce the value obtained if data is stolen. Even if a hacker can access the data, it's important to make sure there is little they can do with it. In other words, **companies need to secure the breach.**

The emergence of the Internet of Things (IoT) will have a huge impact. It will bring new opportunities and convenience, but with so many moving parts, IoT increases the number of attack vectors for cyber criminals. The more access to more data they have, the more creative the attacks. Take for example, the success and intricacy of today's social engineering attacks.

Some of these will have immediate consequences for individuals and companies and others will take longer to identify, giving hackers the time to conduct the most drastic breaches like data integrity attacks. Organizations base their decisions on the data they have access to and often rely heavily on its validity. If hackers or governments can modify the integrity of the data, major business decisions can be manipulated, resulting in significant yet still unknown consequences.

This year, the BLI highlights four major cyber criminal trends:

1. Casting a wider net by going after companies with large numbers of data records thereby maximizing efforts.
2. Using easily-attainable account and identity information as a starting point for high-value targets.
3. Shifting from attacks targeted at financial organizations to infiltrating large data bases such as entertainment and social media sites.
4. Using encryption maliciously by extorting breached organisations and/or their customers, holding their data ransom by making it unreadable.

This year **only 75** of the data breaches (or 4.2% of the total) involved data that had been encrypted in part or in full.

This transition in the hacking community makes it harder for enterprises do determine the implications of attacks. It's important companies take a situational awareness approach to data and identity security by knowing exactly where their data resides, the security categories of the data and a user's access rights to each data category. Companies can no longer assume they will be immune to attacks, but prepare a secure breach environment.

Security executives along with their counterparts in IT and business need to be at the forefront of developing effective programs that level security at multiple levels—particularly the protection of the data itself. By doing this, they can help their organizations protect themselves and their customers.

A NEW MINDSET

2016 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.

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