2017

The Year of Internal Threats and Accidental Data Breaches

Findings from the 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 THE YEAR 2017

2,600,968,280

NUMBER OF BREACH INCIDENTS

1,765

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

55.9%

PERCENTAGE OF DATA BREACHES WHERE ENCRYPTION WAS USED

3.1%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

EVERY DAY
7,125,940

EVERY HOUR
296,914

EVERY MINUTE
4,949

EVERY SECOND
82

A Record Year for Stolen Data

A fair number of data breach trends emerged in 2017. One of the most significant developments of the year was an abundance of poor security practices. Malicious actors were able to hack **Equifax** in the summer of 2017, for example, because the credit bureau failed to improve its security practices after thieves made off with its data in May 2017 and earlier that year. Equifax also didn't have a robust vulnerability management plan in place, allowing criminals to exploit a vulnerability in its website, move laterally across the company's network, and steal hundreds of millions of Americans' personal information.

Poor security practices were also evident in the way multiple organizations mismanaged their Amazon Web Services (AWS) resources. Entities such as the **National Security Agency (NSA)**, the **Pentagon**, and tech giant **Accenture** didn't properly configure their S3 buckets. As a result, members of the public could read and write to sometimes hundreds of gigabytes of exposed data.

Not surprisingly, these incidents along with other consumer breaches reflect enterprises' concern with securing data in the cloud. More than half of enterprises told Gemalto in its *2018 Global Cloud Data Security Study* that they're worried about securing payment information stored in the cloud. 49 percent of respondents said the same about protecting customers' data hosted in the cloud.

Their concern stems in part from the rise of accidental loss as the dominant source of data breaches in 2017. Incidents involving accidental loss increased significantly from under 250 million in 2016 to nearly 2 billion the following year. Consistent with the incidents that struck Equifax and the Pentagon, these events stemmed largely from poor security measures protecting external assets like websites and backup systems as well as misconfigured systems like publicly readable and writable AWS S3 buckets.

Meanwhile, identity theft continues to be a major type of data breach. It was responsible for 682,506,529 compromised records and 1,222 incidents in 2017, marking the greatest number of incidents among all other data breach types. No incident demonstrates the persistence of identity theft as a data breach source better than Equifax. Those responsible for the breach made off with the personal information of 147.7 million U.S. consumers including their names, birth dates, addresses, Social Security Numbers, and driver's license numbers. With those stolen identity details, attackers can apply for lines of credit in their victims' names.

Incidents involving accidental loss and identity theft weren't the only ones to experience growth in 2017. Energy sector attacks returned during the year with sophisticated campaigns like DragonFly 2.0, a malicious email operation which has been attempting to learn about and gain access to energy systems in North America and Europe since at least 2015. Those behind DragonFly 2.0 could use what they've learned in their espionage attacks to disrupt the operations of multiple critical infrastructure systems at targeted organizations.

DATA BREACHES

Integrity-based attacks were also part of the threat scape last year. The integrity component of the **CIA triad** (confidentiality, integrity and availability), which is used by organizations to guide information security policies, can often be overlooked. Organizations are committing more resources to preventing unauthorized information disclosures or distributed denial-of-service (DDoS) campaigns that undermine data's accessibility. However, data manipulation or data integrity attacks are often difficult to identify making them a growing security risk for many organizations, as these type of attacks involve hackers altering anything from sales numbers to intellectual property. Organizations should consider this a significant risk and invest in technology aimed at protecting the integrity of business resources to ensure data isn't tampered with and can still be trusted.

Take crypto-ransomware, for instance. According to Malwarebytes Labs *2017 State of Malware Report*, ransomware detections in 2017 were up 90 percent and 93 percent for businesses and consumers, respectively. Global outbreaks including **WannaCry** and **BadRabbit** drove much of that growth. Even so, statistics for the detection of new ransomware families went down as new threats emerged.

Perhaps more than any other menace, new cryptocurrency-themed attacks defined the second half of the year. Some actors deployed web-based crypto-miners to surreptitiously consume users' CPU and mine digital currency in what are known as "cryptojacking" attacks. Others went after cryptocurrency exchanges and attempted to hack the money, not the data, contained therein. These bad actors' success against a number of marketplaces including **Bithumb**, **Nicehash**, **Youbit**, and **EtherDelta** highlights the need for better security in the cryptocurrency community. Looking ahead, new government regulations could change how many organizations approach digital security. The European Union's General Data Protection Regulation (GDPR) could yield more accurate data breach costs and information about incidents as businesses that handle EU citizens' information work to achieve compliance with the standards. Similar legislation adopted in Australia has already achieved that effect. Within the first month of the Privacy Amendment (Notifiable Data Breaches) Act of 2017 taking effect, Australia's OAIC received 31 notifications of data breaches, which includes an incident involving the shipping company Svizter Australia.

At the same time, incidents like the **SEC hack** and the **Kerala Motor Vehicles Department database compromise** indicates that government bodies should consider stepping up their own protections.

The following section presents some of the most notable data breaches that occurred in 2017. It includes the number of compromised records, type of breach, and risk assessment score for each of the featured events. The score is calculated based on factors such as the number of records breached, source of breach, and how the information was used.

These are just some of the trends to emerge from a comprehensive analysis of security breaches. To create the report, **Gemalto**, a leading global provider of digital security solutions, collected extensive publicly-available information about data breaches around the globe. This information is aggregated into the **Breach Level Index**, a database that Gemalto maintains on worldwide data breaches.

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

TOP NOTABLE BREACHES 2017 YEAR IN REVIEW

A score of 1 to 2.9 is 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 Breach Level Index is to demonstrate that not all breaches have the same impacts on organizations and amount of risk. Many of the top breaches fell into the identity theft category.

Equifax

RECORDS: **143,000,000**
TYPE: **Identity Theft**
SCORE: **10.0**

Malicious actors infiltrated Equifax's systems by exploiting a weak point in the credit bureau's website software. According to The New York Times, the hack granted them access to sensitive files in the credit bureau's system from mid-May to July. Equifax and security consultants believe the malicious outsiders might have compromised the names, dates of birth, Social Security Numbers, and other personal information of 147.7 million U.S. consumers in that span of time. Given its potential scope, the Equifax breach received a Breach Level Index score of 10.

River City Media

RECORDS: **1,340,000,000**
TYPE: **Nuisance**
SCORE: **9.8**

An email marketing organization called River City Media failed to properly configure its Rsync backups, thereby making its data publicly viewable online. In examining the data, researchers discovered that the organization had created a database of 1.34 billion email addresses that it sent spam mail in the form of "offers." The breach, which received a Breach Level Index rating of 9.8, also exposed customers' names and physical addresses along with several thousands of email addresses used by the company to avoid anti-spam filters.

Deep Root Analytics / Republican National Committee (RNC)

RECORDS: **198,000,000**
TYPE: **Identity Theft**
SCORE: **9.6**

A data firm contracted by the Republican National Committee, Deep Root Analytics stored personal information on nearly all 200 million American voters for two weeks on Amazon's cloud without proper password protections. Researcher Chris Vickery found that the misconfiguration exposed more than a terabyte of personal details including names, home addresses, phone numbers, and dates of birth. This accidental loss incident earned a Breach Level Index score of 9.8.

Alteryx

RECORDS: **123,000,000**
TYPE: **Identity Theft**
SCORE: **9.4**

In December, Vickery found an Amazon Web Services storage bucket left open to the public by marketing analytics firm Alteryx. The exposure, which merited a 9.4 Breach Level Index ranking, exposed the sensitive information of more than 120 million American households such as the names of residents, income, mortgage rates, and even residents' interests/hobbies.

Center for Election Systems at Kennesaw State University

RECORDS: **7,500,000**
TYPE: **Identity Theft**
SCORE: **9.1**

Center for Election Systems at Kennesaw State University. On 2 March 2017, Kennesaw State University contacted the FBI about a breach at its Center for Election Systems. The event could have compromised as many as 7.5 million Georgians' voter records. For that reason, the security incident received a Breach Level Index score of 9.1.

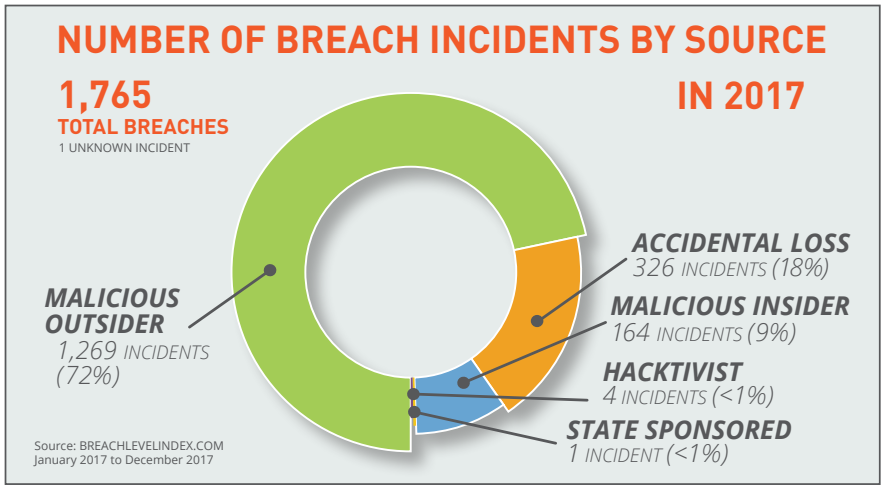
LEADING SOURCES OF DATA BREACHES

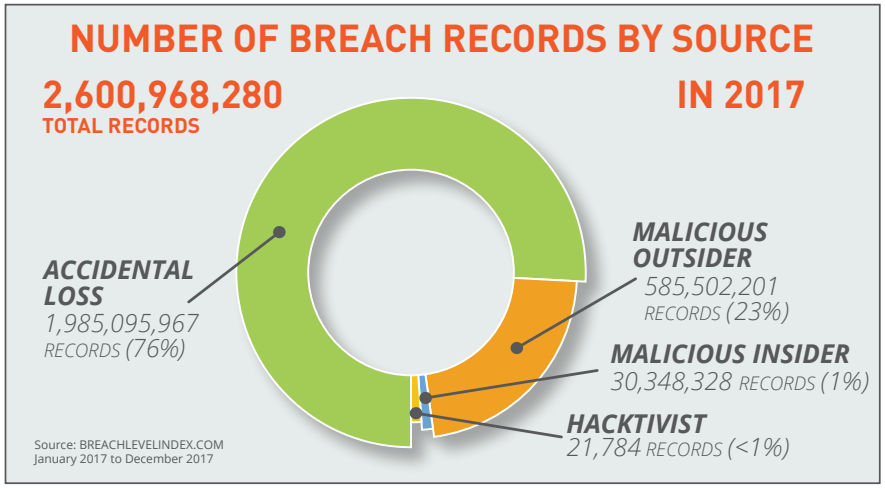
Accidental Loss Leads the Way

No other data breach source came close to **accidental loss** and its 580 percent increase to almost 2 billion compromised records in 2017. The next highest source was **malicious outsider**, which dropped by 44.6 percent from just over 1 billion records in 2016 to just over 585 million breached records a year later. To its credit, malicious outsider produced the greatest number of incidents at 1,269 - an even 5 percent decline from 1,336 over the previous year.

In fact, the only data breach source other than accidental loss that exhibited any growth between 2016 and 2017 was **malicious insider**. Comparatively, it was a mere uptick: a 117.3 percent increase from 13,963,040 to 30,348,328. At the same time, the number of malicious insider incidents declined 8.4 percent from 179 to 164.

All other sources declined by 100 percent or close to it. Records compromised by **state-sponsored** attacks dropped from 10,797,581 to 0, with incidents falling from 20 to 1. Breaches with **unknown** sources carried similar losses: a decline of compromised records from 950,000 to 0 and of incidents from 4 to 1. **Hacktivist** attacks fared a fraction of a fraction better, exhibiting a 99.8 percent decline from 12,371,864 records breached to 21,784 along with a similar decrease in incidents from 49 to 4.

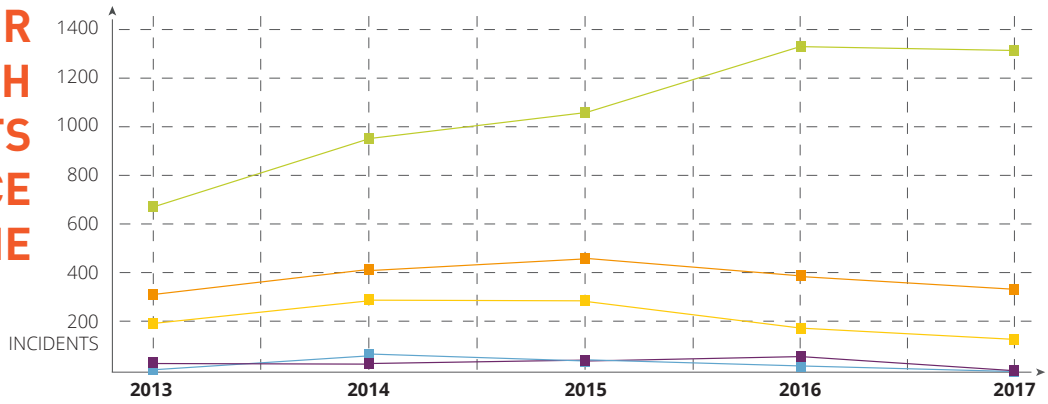




DATA BREACHES BY SOURCE

2017 YEAR IN REVIEW

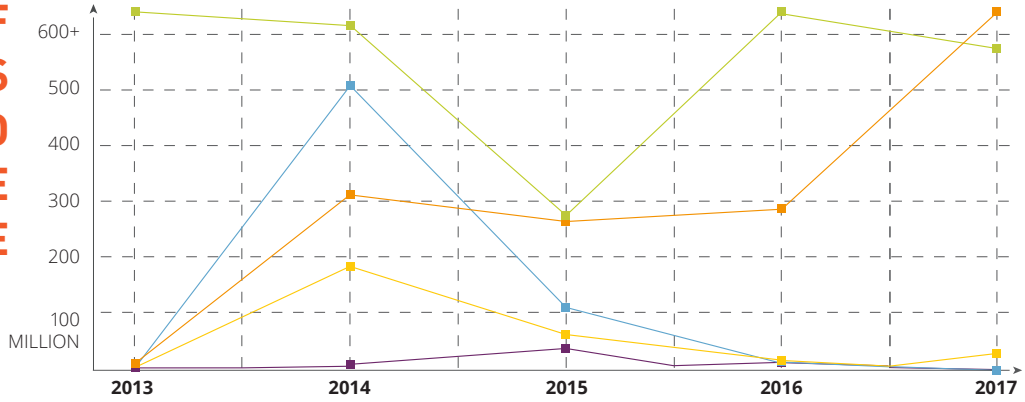
NUMBER OF BREACH INCIDENTS BY SOURCE OVER TIME



BREACH SOURCE	2013	2014	2015	2016	2017
Malicious Outsider	662	955	1,087	1,336	1,269
Accidental Loss	302	413	442	393	326
Malicious Insider	195	290	278	179	164
Hacktivist	27	20	36	49	4
State Sponsored	12	61	36	20	1
Unknown	19	4	4	4	1
TOTALS	1,217	1,743	1,883	1,981	1,765

Source: BREACHLEVELINDEX.COM

NUMBER OF RECORDS BREACHED BY SOURCE OVER TIME



BREACH SOURCE	2013	2014	2015	2016	2017
Malicious Outsider	2,081,285,434	674,544,208	274,762,361	1,057,189,069	585,502,201
Accidental Loss	15,068,756	309,823,689	265,209,847	292,246,026	1,985,095,967
Malicious Insider	10,371,810	185,738,742	64,791,635	13,963,040	30,348,328
Hacktivist	875,946	8,182,103	30,573,822	12,371,864	21,784
State Sponsored	165,053	509,928,563	108,076,636	10,797,581	0
Unknown	77,525	1,307	591	950,000	0
TOTALS	2,107,844,524	1,688,218,612	743,414,892	1,387,517,580	2,600,968,280

Source: BREACHLEVELINDEX.COM

TYPES OF DATA COMPROMISED

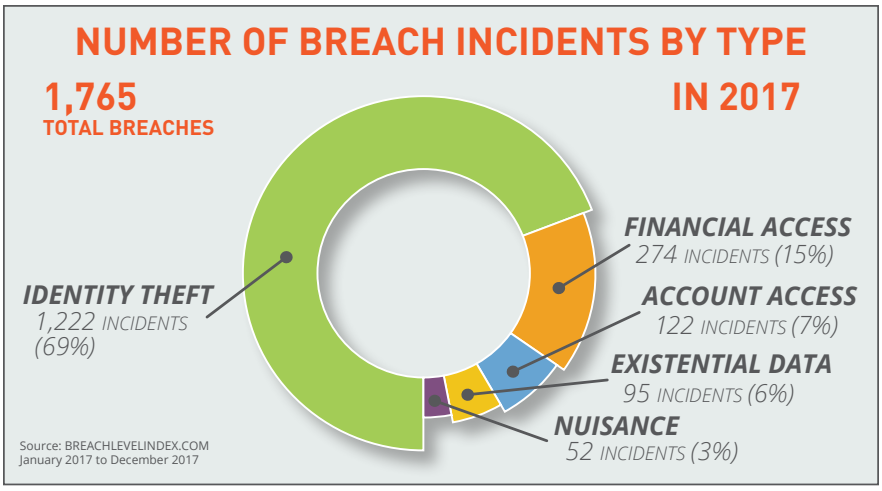
Data Breaches a Big Nuisance

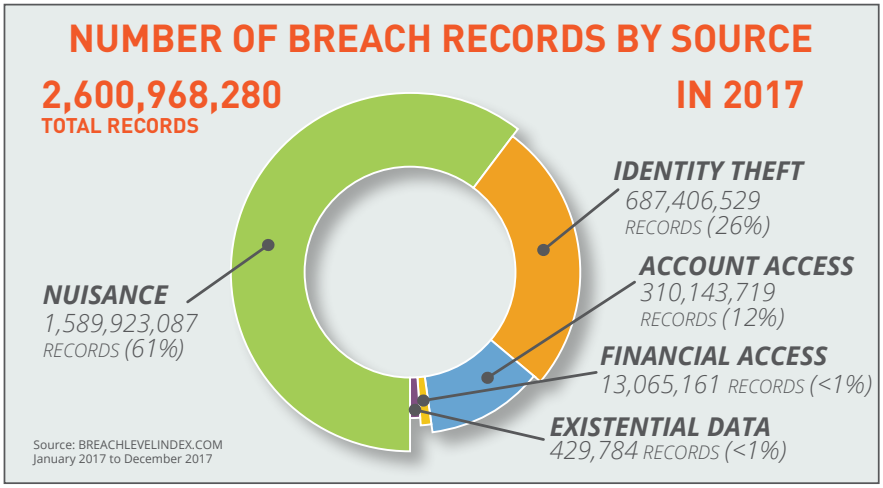
Nuisance was the most common type of data breach in 2017. In the span of one year, the number of records compromised by these types of incidents increased by 561 percent from more than 240 million to more than 1.5 billion noted. Nuisance data breaches didn't grow in number to match those figures, however. In fact, these events decreased by more than 50 percent from 107 in 2016 to 52 the following year.

In terms of growth, data breaches consisting of **financial access** and **identity theft** also saw impressive gains. The former type of incident went up 189.1 percent from 4,519,712 compromised records to 13,065,161 in the span of a year. During that same time frame, the latter jumped up 73.2 percent from 396,829,721 records to 687,406,529. There were just 274 incidents of financial access in 2017, a 22 percent decline from 2016. **Identity theft** also declined 1.5% from 1,240 to 1,222 instances. Even so, it still marked the greatest number of incidents among all other data breach types.

Gemalto observed a much more significant decrease with **existential data** breaches. Those incidents didn't diminish much in number; they went down five percent from 100 to 95. But the number of records breached plummeted 99.9 percent from 415,460,666 to 429,784.

Meanwhile, **account access** breaches experienced more modest losses: a 6 percent drop in the number of records from 329,998,234 to 310,143,719 and a 33 percent fall in the number of incidents from 182 to 122.

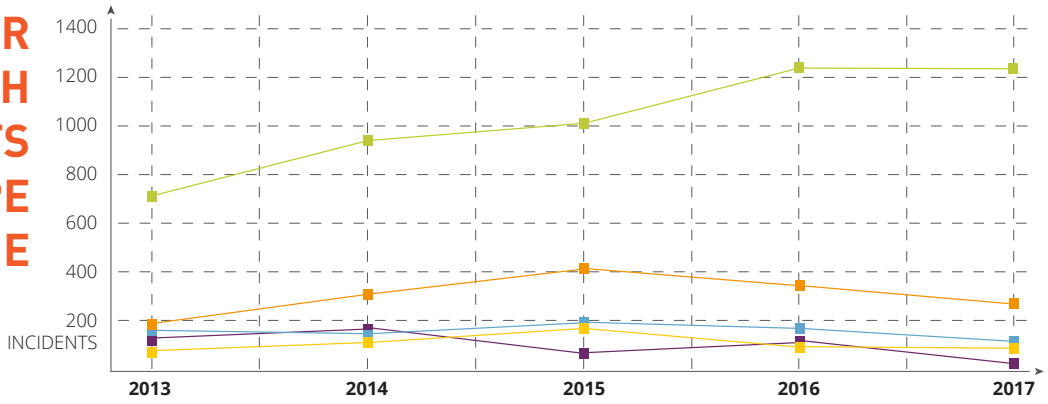




DATA BREACHES BY TYPE

2017 YEAR IN REVIEW

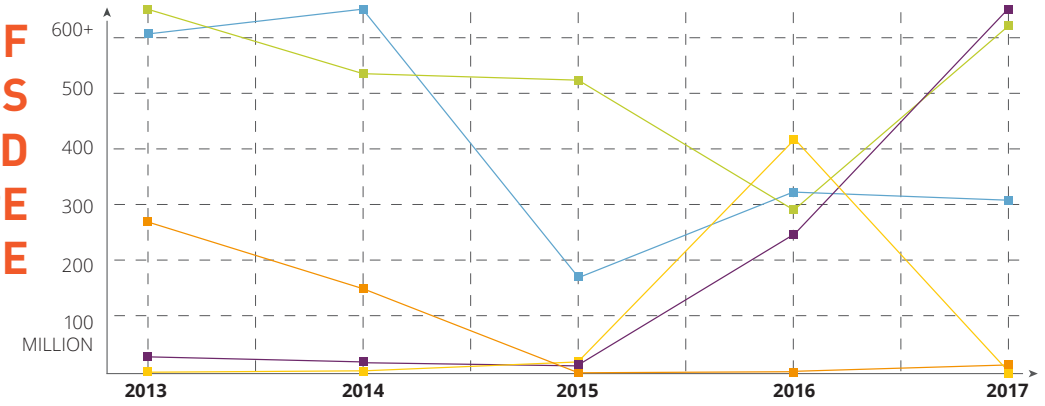
NUMBER OF BREACH INCIDENTS BY TYPE OVER TIME



TYPE OF BREACH	2013	2014	2015	2016	2017
Identity Theft	715	937	1,014	1,240	1,222
Financial Access	193	303	413	352	274
Account Access	139	171	199	182	122
Existential Data	57	158	186	100	95
Nuisance	113	174	71	107	52
TOTALS	1,217	1,743	1,883	1,981	1,765

Source: BREACHLEVELINDEX.COM

NUMBER OF RECORDS BREACHED BY TYPE OVER TIME



TYPE OF BREACH	2013	2014	2015	2016	2017
Nuisance	28,824,301	27,961,192	15,300,822	240,709,247	1,589,923,087
Identity Theft	1,189,281,505	535,324,198	526,853,396	292,246,026	687,406,529
Account Access	609,689,524	969,472,243	171,873,091	329,998,234	310,143,719
Financial Access	274,460,093	152,114,562	4,102,305	4,519,712	13,065,161
Existential Data	5,589,101	3,346,417	25,285,278	415,460,666	429,784
TOTALS	2,107,844,524	1,688,218,612	743,414,892	1,387,517,580	2,600,968,280

Source: BREACHLEVELINDEX.COM

COMPARING THE INDUSTRIES

From an industry perspective, the greatest number of records compromised between 2016 and 2017 originated from organizations in economic sectors classified as "**other**." These "other" industries racked up over 1.3 billion breached records in 2017, up from more than 86 million the year before - more than a 1,400 percent increase! That surge notwithstanding, the number of incidents declined in those segments by 57.5 percent from 160 to 68.

Astonishingly, **professional services** and **social media** saw an even greater rate of growth in their number of compromised records over the course of the year. Breached accounts for the former industry increased to more than 1 million from 0. Its number of incidents also experienced monumental gains, swelling from just one case in 2016 to 92 the following year. As for the former, compromised documents pertaining to social media expanded greatly percent from just 1,489 to close to 20 million, whereas the number of incidents grew from 2 to 9.

Other sectors also experienced a notable influx of breached records. For example, **industrial** organizations saw the number of compromised accounts shoot up to 2,394,448 from 67,210. Incidents also became more numerous between 2016 and 2017 from 32 to 60 - a surge of 87.5 percent.

During that same time period, enterprises specializing in **financial services** weathered an increase from 13,364,697 to 235,563,765, with the number of incidents decreasing by nearly 10 percent from 241 to 219. The rise of breached records in **education** was less than half that of financial services at 652 percent, ballooning from approximately 4.5 million to nearly 33.5 million. Incidents in that sector grew about 20 percent from 166 to 199.

A few other industries registered modest growth in their breached account totals. These include the following sectors:

Government: An 18.7 percent rise in records from 391,795,340 to 465,014,660 occurred in governmental agencies, with incidents declining more than a third from 289 to 193.

Healthcare: Compromised accounts grew 27.4 percent to 33,717,772 from 26,467,715. Incidents decreased by 11.3 percent during that same period from 531 to 471. Even so, healthcare organizations encountered the greatest number of breaches among all other industries in 2017.

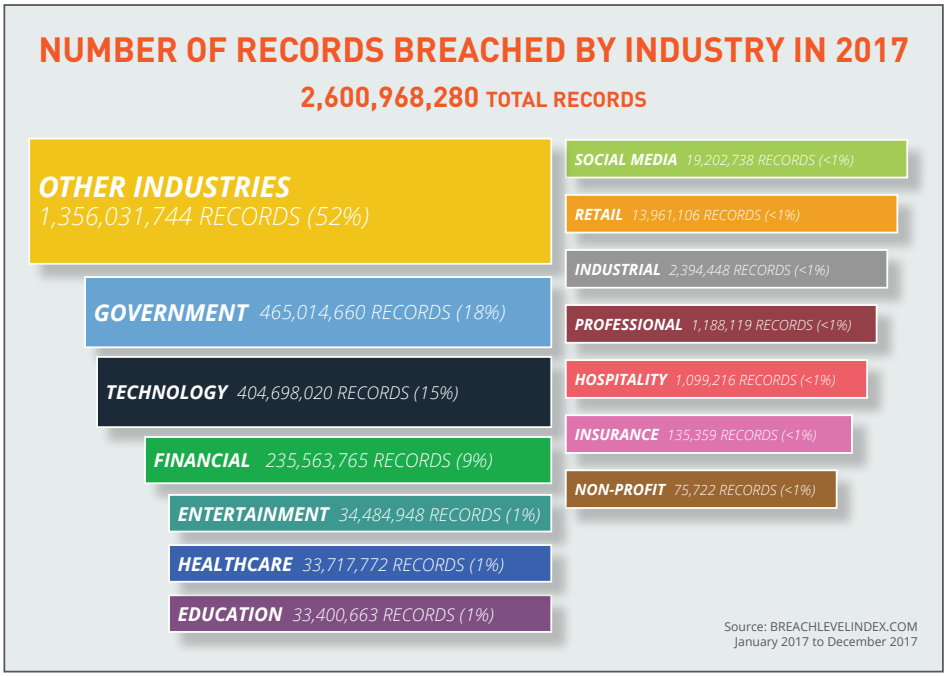
Technology: With a 3 percent increase in breached files in the technology sector, numbers went up only slightly from 392,727,945 to 404,698,020. Breaches involving technology providers went down during that same period from 203 to 130.

There were plenty of industries where the total breached records actually fell but the number of incidents rose. **Entertainment's** compromised accounts slid 91.8 percent from

COMPARING THE INDUSTRIES

2017 YEAR IN REVIEW

419,864,632 - the highest of any industry in 2016 - to 34,484,948 in 2017. But incidents grew during that same period by 48.4 percent from 31 to 46. Similarly, exposed documents in **hospitality** dropped 88.5 percent to 1,099,216 from 9,568,998, yet events rose slightly by 2.9 percent from 35 to 36. And then there's **insurance**, whose total number of breached records dipped by 98.5 percent from 9,307,242 to 135,359 and whose incidents increased by nearly a half from 15 to 22.



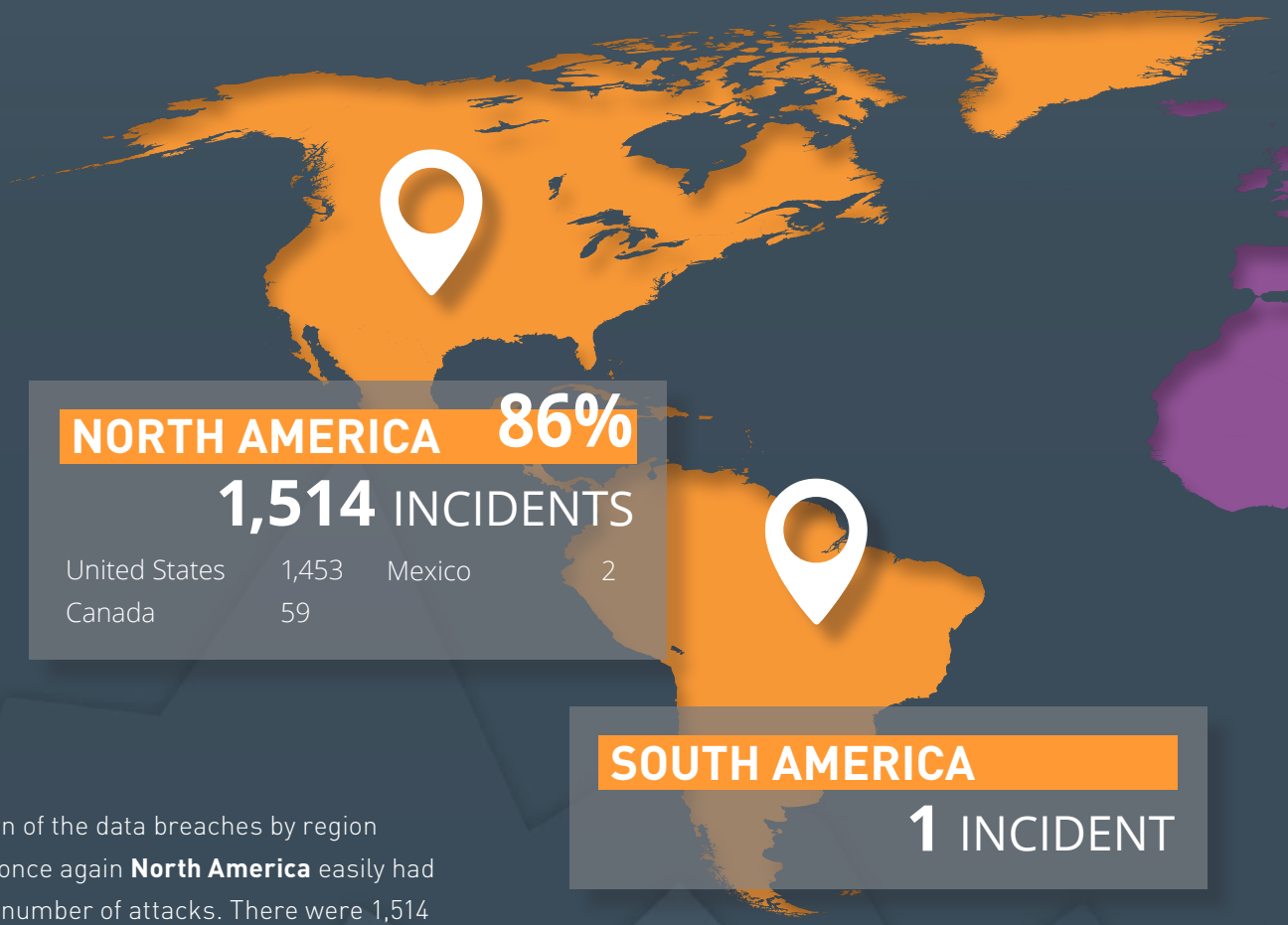
Last but not least, two industries saw the number of breaches and compromised records both decrease between 2016 and 2017. The first was **non-profit** organizations, with exposed accounts falling 8.9 percent from 83,128 to 75,722 and incidents experiencing a quarter drop from 28 to 21. The second was **retail**. Breached files and events for that industry plunged 57.9 percent from 33,168,943 to 13,961,106 and 19.4 percent from 247 to 199, respectively.

NUMBER OF BREACH INCIDENTS BY INDUSTRY OVER TIME

INDUSTRY	2013	2014	2015	2016	2017
Healthcare	346	449	451	531	471
Financial Services	166	213	276	241	219
Retail	97	197	240	247	199
Education	36	174	166	166	199
Government	196	293	299	289	193
Technology	112	140	124	203	130
Professional Services	-	1	1	1	92
Other Industries	263	275	316	160	68
Industrial	-	-	-	32	60
Entertainment	-	-	5	31	46
Hospitality	1	1	2	35	36
Insurance	-	-	2	15	22
Non-Profit	-	-	-	28	21
Social Media	-	1	2	2	9
TOTALS	1,217	1,743	1,883	1,981	1,765

Source: BREACHLEVELINDEX.COM

THE GEOGRAPHICAL VIEW

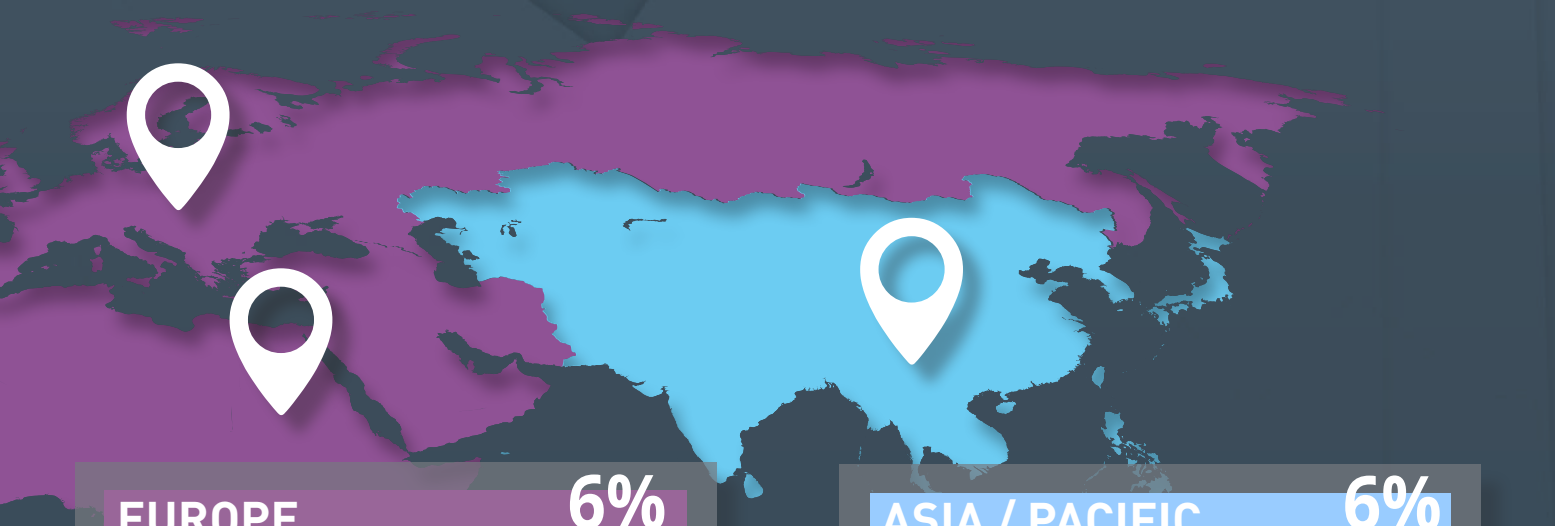


A breakdown of the data breaches by region shows that once again **North America** easily had the highest number of attacks. There were 1,514 breaches in the U.S., Canada, Mexico, and Central America, 86% of all the breaches that occurred worldwide. That was down slightly from 2016 amount of 1,608. The number of records stolen in the North American breaches was just over 2 billion, or 78% of the total. That almost doubled the record count from the previous year.

Organizations in **Europe** were hit with 112 breaches (6% of the total), down 31% from last year. These attacks resulted in the theft of 36 million records, an 80% decline.

The **Asia-Pacific** region experienced 113 data breaches in 2017, accounting for 7% of the total and down 24% from 2016. Other regions of the world experienced much smaller numbers of breaches. **Africa** had 10 data breaches, down 44%, and the **Middle East** had six breaches, down 74%. Most of these regions will see an 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 May 25th, 2018.

2017
YEAR IN REVIEW



EUROPE 6%

112 INCIDENTS

United Kingdom	80	Czech Republic	2
Ireland	7	Finland	2
Netherlands	7	Malta	2
Italy	4	Sweden	2

ASIA / PACIFIC 6%

113 INCIDENTS

Australia	40	South Korea	5
India	29	Hong Kong	3
New Zealand	10	Malaysia	3
Singapore	10	Japan	2
China	5		

MIDDLE EAST / AFRICA 1%

16 INCIDENTS

South Africa	7	Kenya	2
Middle East	6		

GLOBAL

9 INCIDENTS

SECURITY LESSONS FROM 2017

Overall, Gemalto detected an 11 percent drop in the number of data breaches from 1,981 in 2016 to 1,765 in 2017. In spite of that decline, **Breach Level Index data suggests that security incidents are getting faster and larger in scope.** The total number of records breached every day, hour, minute, and second tracked by Gemalto nearly doubled in the span of a year. The aggregate number of breached records saw similar growth from 1,387,517,580 to 2,600,968,280, an 87.5 percent increase from 2016 to 2017. That's the first time the total number of records detected by BLI over a calendar year has exceeded 2 billion.

It should also be pointed out that breaches with an unknown number of records increased from 936 to just 987, which demonstrates how hard it is to get an accurate picture of the number of data records and accounts that are compromised every year.

The data collected by Gemalto's BLI highlights three trends from 2017 that organizations should consider going into 2018. These are as follows:

- A lack of proper safeguards and training in the form of accidental data loss produced billions of data breaches.
- Relatively few data breaches occurred where encryption was used. In 2017, there were 55 such incidents, down 33.7 percent from 83 occurrences in 2016. These events constituted 3.12 percent and 4.19 percent of the total breaches for their respective years. The number of records also fell by 52.7 percent between 2016 from 75,558,319 (5.45 percent of the total records) to 26,954,314 (1.04 percent of the total records).
- Malicious outsiders compromised hundreds of millions of records in security incidents involving identity theft and account access.

Given those trends, organizations can and should take several steps to better protect themselves against a data breach. First, they should take control and invest more in security. As Jim Kennedy recommends in an article for CSO, enterprises need to shift away from external contractors and towards internal employees who can implement encryption, access controls, authentication, and other security measures.

Given the prevalence of AWS storage breaches, these safeguards should include measures for the cloud. That's a wise move considering how many organizations use cloud-based resources.

According to Gemalto's 2018 Global Cloud Data Security Study, 79 percent of IT professionals say cloud computing applications are important to business processes, estimating that the cloud meets approximately 39 percent of their organizations' current IT and data processing needs. But organizations aren't doing all they can to secure their cloud-based data. Just 47 percent of respondents told Gemalto that their employer uses encryption, whereas only half say multi-factor authentication is in place for employee access to the cloud. Companies should make the move to adopt those measures in the cloud.

Once they've set up those safeguards, companies need to invest more in their employees with ongoing training on access control. With a robust security culture in place, employees can make the right security decisions to serve as an organization's front line of defense against data breaches and other digital threats.

Lastly, **organizations need to prepare for what many consider to be the inevitability of a digital attack.** They can do so by prioritizing their IT assets and determining what the business impact of an attack would be on those resources. Using that knowledge, organizations can craft a thorough digital security strategy replete with incident response plans that specifically suit their needs.

A NEW MINDSET

2017
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 safenet.gemalto.com.