DATA BREACH DISCOVERIES FROM THE

BREACH LEVEL INDEX

Data Privacy and New Regulations Take Center Stage

2018

FIRST HALF REVIEW

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 FIRST HALF OF 2018

4,553,172,708

NUMBER OF BREACH INCIDENTS

945

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

20%

PERCENTAGE OF DATA BREACHES WHERE ENCRYPTION WAS USED

2.2%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

25,155,650 EVERY DAY

1,048,152 EVERY HOUR

17,469 EVERY MINUTE

291 EVERY SECOND

Privacy Takes Center Stage

A number of important data breach trends emerged in the first half of 2018. One of the most notable of these developments was the introduction of new data protection regulations including the European Union's *General Data Protection Regulation (GDPR)*, New York's *Cybersecurity Requirements for Financial Services Companies* and Australia's *Notifiable Data Breach (NDB)* scheme. The rationale behind passing these standards is to help organizations better protect customers' privacy and security by design. But the regulations aren't without their drawbacks for businesses. Not only do they impose additional costs in terms of compliance; they also lead to an increase in the number of reported breaches.

For instance, in the first three weeks of the NDB scheme, the *Office of the Australian Information Commissioner (OAIC)* received 31 data breach notifications. By the end of the Q2 2018, this number had jumped up to 305, thereby almost tripling the amount (114 notifications) submitted to the OAIC for the entire 2016-2017 fiscal year under the previous reporting scheme. Among the incidents disclosed to the OAIC in the second quarter of 2018 was a data breach at **PageUp**. This security event led to a flurry of data breach notices as clients of the HR software provider worked to protect their customers.

Given the rationale for GDPR and other data protection regulations, it's no wonder that privacy took center stage in the first half of 2018. That was the case especially with instances where companies violated users' privacy. Such was the case in a data scandal where the political consulting firm **Cambridge Analytica** improperly harvested the data of 87 million **Facebook** users. A short time afterward, the social networking website revealed that malicious actors might have abused its search and account recovery mechanisms to scrape the public profiles of "most people on Facebook," meaning as many as two billion users.

Given the rationale for GDPR and other data protection regulations, it's no wonder that privacy took center stage in the first half of 2018.

Incidents such as those experienced by Facebook concern many users not just because of the damage done to their privacy. In the wrong hands, bad actors can use information scraped from Facebook public profiles and other sources to commit identity theft. Digital attackers have already demonstrated a proclivity for these types of security incidents, with identity theft dominating 65 percent of all data breaches observed in the first half of 2018 including security incidents involving the **Government of India** and **Exactis**. Once in possession of people's personal details, identity thieves can monetize that information on underground marketplaces. They can also leverage them for conducting identity fraud along with other subsequent attacks.

In terms of data breach sources, malicious outsiders and accidental loss were at the top of the list in the first half of 2018. Those forces accounted for some of the biggest security incidents reported including **Twitter** and **Under Armour**.

BREACH LEVEL INDEX

DATA BREACHES

Accidental loss in particular, was the leading factor behind several breaches where data records were disclosed because organizations didn't take proper action to secure their cloud-based assets. One of the largest of these leaks involved the exposure of 48 million records belonging to **LocalBlox**, a personal and business data search service. Then there was Bongo International, a company acquired by **FedEx** in 2014 which misconfigured an Amazon S3 bucket containing 119,000 scanned documents including individual passports, driving licenses and security IDs.

The report analyzes the data in terms of the number of breaches, the number of data records compromised and data breaches by the source of the breach, type of breach, industry and geographic location.

2018: More Data Stolen Than Ever Before

Overall, the total number of records compromised in the first half of 2018 was 4,553,172,708. That figure marks an increase of 133 percent over H1 2017. Not surprisingly, the amounts of records breached every day, hour, minute and second also surpassed the totals observed a year earlier. What is remarkable is that all of these figures more than doubled between 2017 and 2018.

Surprisingly, there were just 945 security incidents reported in the first half of 2018. That's 18.7 percent fewer than the 1,162 breaches disclosed in H1 2017. Of those incidents, there were just 21 data breaches where encryption was reportedly used on the data in whole or in part. That's less than half the figure for the previous year. These fewer incidents exposed almost three times the number of records in H1 2018 (42,740,464) as opposed to H1 2017 (16,975,765). At the same time, the number of breaches involving an unknown number of records decreased from 667 to 189 in the first half of 2018.

The following section presents some of the most notable data breaches that occurred in H1 2018. 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 verified publicly-available information and news reports on data breaches around the globe. This information is aggregated into the **Breach Level Index**, a database that Gemalto maintains on worldwide data breaches.

TOP NOTABLE BREACHES 2018

FIRST HALF REVIEW

A score of 1 to 2.9 is minimal risk, 3 to 4.9 is moderate and 5 to 6.9 is critical. 7 to 8.9 is severe, and 9 to 10 is catastrophic. The point of the scoring system is to demonstrate that not all breaches have the same impact on organizations and amount of risk. Many of the top breaches fell into the malicious outsider and accidental loss categories.

Facebook

RECORDS BREACHED
2,200,000,000
TYPE OF BREACH
Identity Theft
SOURCE OF BREACH
Malicious Outsider
LOCATION
United States
INDUSTRY
Social Media
RISK SCORE
10.0

Facebook revealed that malicious actors could have abused its search and account recovery capabilities to scrape public profile information from most of its more than 2 billion users. The social networking platform discovered that bad actors had the option of submitting phone numbers and email addresses to locate users' public profiles and obtain personal information off them. As Facebook's CTO Mike Schroepfer explained at the time, "Given the scale and sophistication of the activity we've seen, we believe most people on Facebook [over 2 billion users] could have had their public profile scraped in this way." The tech giant responded by disabling the feature and changing its account recovery process to reduce the risk of scraping.

Aadhaar

RECORDS BREACHED
1,200,000,000
TYPE OF BREACH
Identity Theft
SOURCE OF BREACH
Malicious Outsider
LOCATION
India
INDUSTRY
Government
RISK SCORE
10.0

An anonymous service allowed anyone with 500 rupees to access all 1.2 billion Indian citizens' personal information. In January 2018, the **Tribune News Service** paid to access a service being offered by anonymous sellers over WhatsApp. Reporters found they could use the service to enter any Aadhaar number, a 12-digit unique identifier assigned to every Indian citizen, and retrieve personal information stored by the Unique Identification Authority of India on any of India's 1.1 billion citizens including their name, address, photo, phone number and email address. An additional 300 rupees yielded access to software through which anyone could print an ID card for any Aadhaar number.

Exactis

RECORDS BREACHED
340,000,000
TYPE OF BREACH
Identity Theft
SOURCE OF BREACH
Accidental Loss
LOCATION
United States
INDUSTRY
Other
RISK SCORE
9.1

Florida-based marketing and data aggregation firm Exactis left a database containing 340 million individual records unprotected on the web. **Security researcher Vinny Troia** discovered in June 2018 that Exactis had left the database exposed on a publicly accessible server. The database contained two terabytes of information that included the personal details of hundreds of millions of Americans and businesses including consumers' email addresses, physical addresses, phone numbers and other extremely sensitive information like the names and genders of their children. It's unknown how many U.S. individuals the breach exposed, but 340 million individual records were stored within the database at the time of discovery.

Under Armour

RECORDS BREACHED
150,000,000
TYPE OF BREACH
Account Access
SOURCE OF BREACH
Malicious Outsider
LOCATION
United States
INDUSTRY
Retail
RISK SCORE
9.1

An attacker gained unauthorized access to software owned by Under Armour and in so doing compromised as many as 150 million people's account information. On March 25th, the American apparel manufacturer learned that someone had gained unauthorized access to **MyFitnessPal**, its platform which tracks users' diet and exercise. According to **CNBC**, those responsible accessed individuals' usernames, email addresses and hashed passwords. They did not expose users' payment information, as Under Armour processes this data separately. Nor did the unauthorized individual(s) compromise users' Social Security Numbers or driver's license numbers, as Under Armour clarified that it doesn't collect those or any other government identifiers.

LEADING SOURCES OF DATA BREACHES

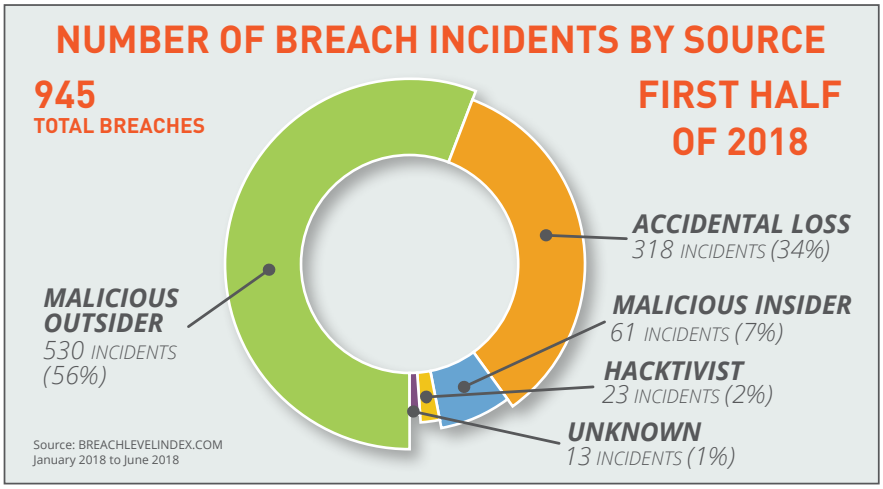
Malicious Outsiders at the Helm

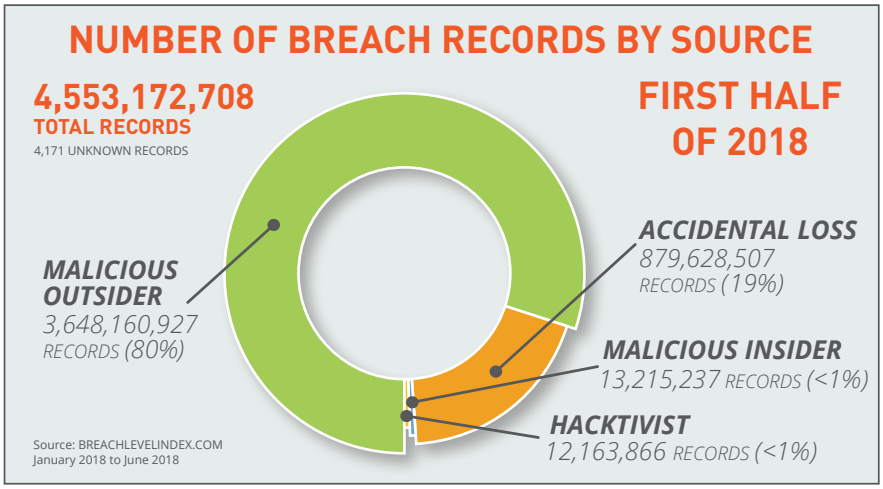
No other source of data breaches came close to **malicious outsiders** in the first half of 2018. The number of records exposed by external attackers rose by 1,294 percent to 3,648,160,927 records breached. Such growth defied the 38 percent decline in the total number of incidents involving malicious outsiders to 530 events.

The number of records compromised by malicious outsiders in H1 2018 easily beat out the previous year's leading data breach source: **accidental loss**. In the first half of 2017, mistakes and misconfigurations were responsible for 1,660,677,295 exposed records. A year later, the number of files exposed by accidental loss dropped by 47 percent to 879,628,507, making it the second leading data breach source for 2018 with 318 incidents.

Compared to malicious outsiders and accidental loss, **hacktivists** compromised fewer records and were responsible for fewer incidents in H1 2018. But they still had a good year. There were 23 incidents of hacktivism, representing a 1,050 percent increase over the previous year. Additionally, the number of records compromised grew from 70,000 to more than 13 million. These findings suggest that hacktivists are fine-tuning their attacks to expose more records at a smaller number of lucrative targets.

By contrast, **malicious insiders** were quieter in H1 2018 compared to the previous year. The number of records they compromised decreased 60 percent to just over 12 million. Similarly, the number of incidents involving malicious insiders was down 45 percent at just 61.

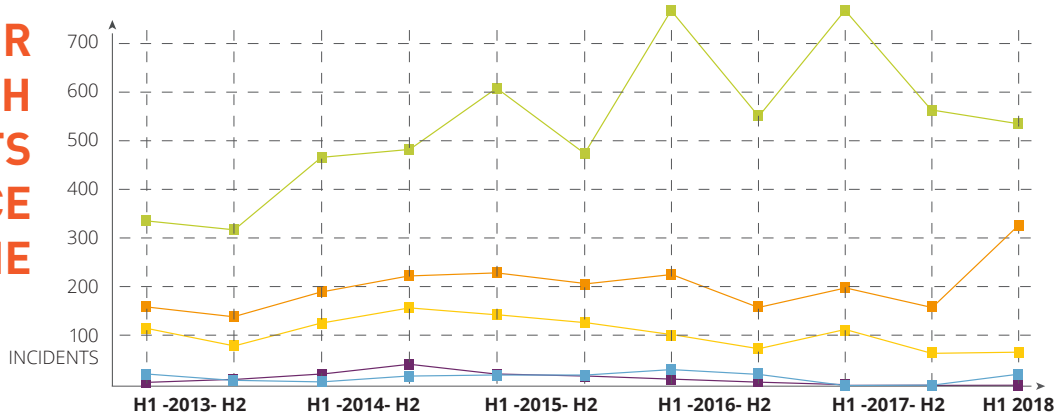




DATA BREACHES BY SOURCE

2018 FIRST HALF REVIEW

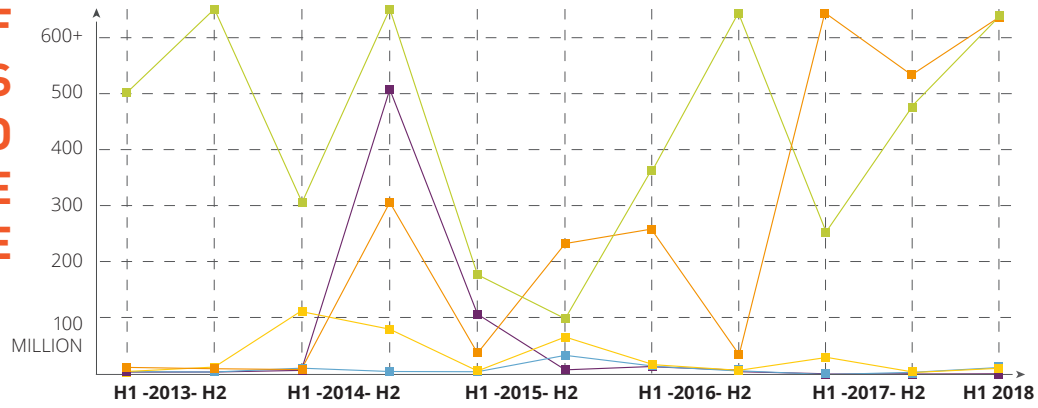
NUMBER OF BREACH INCIDENTS BY SOURCE OVER TIME



BREACH SOURCE	2013		2014		2015		2016		2017		2018
	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1
Malicious Outsider	342	319	472	484	611	478	785	558	849	567	530
Accidental Loss	162	142	192	223	231	213	232	164	199	166	318
Malicious Insider	116	79	130	160	150	128	100	80	110	62	61
Hacktivist	20	7	4	16	18	18	31	19	2	3	23
State Sponsored	3	9	20	41	20	16	13	7	1	0	0
Unknown	16	3	4	0	2	2	2	2	1	0	13
TOTALS	659	559	822	924	1,032	855	1,163	830	1,162	798	945

Source: BREACHLEVELINDEX.COM

NUMBER OF RECORDS BREACHED BY SOURCE OVER TIME



BREACH SOURCE	2013		2014		2015		2016		2017		2018
	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1
Malicious Outsider	502,709,463	1,578,575,971	305,090,925	1,569,453,283	175,545,401	99,259,842	369,960,152	687,838,769	261,694,208	481,540,646	3,648,160,927
Accidental Loss	8,488,082	6,702,567	4,771,897	305,300,000	33,977,717	231,236,930	258,763,768	33,498,745	1,660,677,295	529,347,310	879,628,507
Hacktivist	777,216	98,730	7,000,096	1,182,007	561,918	30,011,904	11,495,885	918,179	70,000	1,784	13,215,237
Malicious Insider	1,150,087	9,221,723	108,770,712	76,968,030	2,006,460	62,785,175	13,484,124	483,437	30,227,855	131,366	12,163,866
State Sponsored	38	165,015	3,016,499	506,912,064	104,009,225	4,067,411	10,355,381	442,200	0	0	0
Unknown	72,780	4,745	1,307	0	391	200	950,000	0	0	0	4,171
TOTALS	513,197,666	1,594,768,751	428,651,436	2,459,815,384	316,101,112	427,361,462	665,009,310	723,181,330	1,952,669,358	1,011,021,106	4,553,172,708

Source: BREACHLEVELINDEX.COM

TYPES OF DATA COMPROMISED

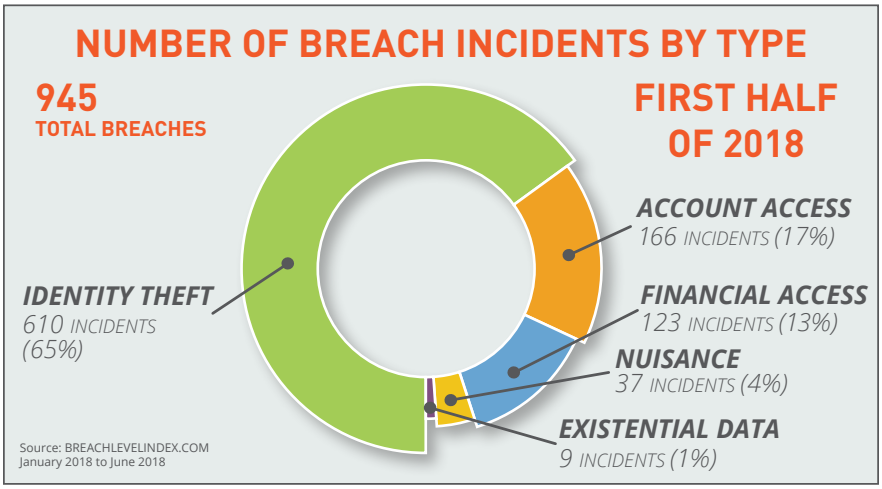
The Domination of Identity Theft

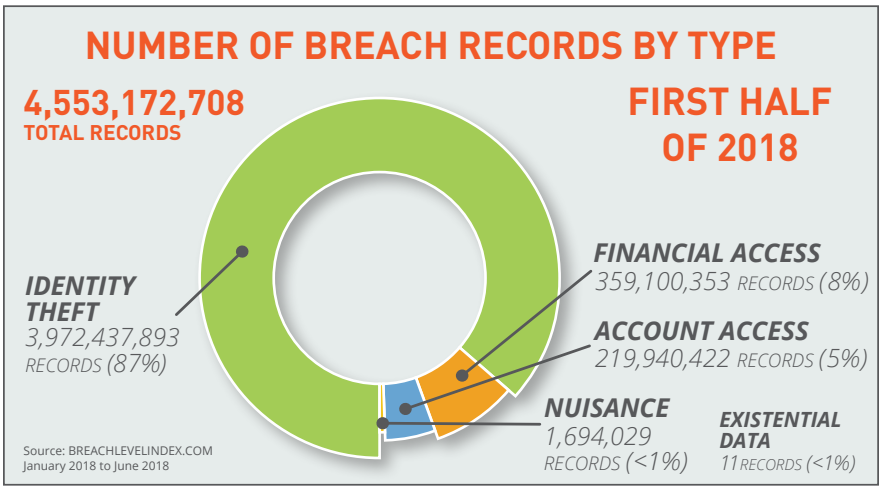
Identity theft was once again the most prevalent data breach type tracked by the BLI. It accounted for 3,972,437,893 compromised records — approximately 87.2 percent of the accounts breached in H1 2018. This number also represents a massive growth of 1,128 percent for identity theft over the previous year. The number of incidents involving identity theft decreased by more than a quarter to 610, which was still the greatest number of events for any data breach type recorded by the BLI.

The next most prevalent types of data breaches were **financial access** and **account access**. Financial access increased its reach by more than 13,000 percent to 359,100,353 compromised records. This data exposure occurred across just 123 incidents, representing a drop by 28.1 percent over H1 2017. By comparison, account access had a more modest gain of 161.7 percent to 219,940,422 compromised records, while the number of incidents also increased by 124.3 percent to 166.

Nuisance, the data breach type which held at the top spot in H1 2017 at more than 1.5 billion compromised records, plunged nearly 100 percent to 1,694,029.

This rate of loss was almost identical for **existential data**, or sensitive company assets like intellectual property. The number of breached records containing this type of data fell from 425,284 to 11. Even so, incidents involving nuisance grew by more than three-quarters to 37, while breaches of existential data dipped 87 percent from 70 to 9.

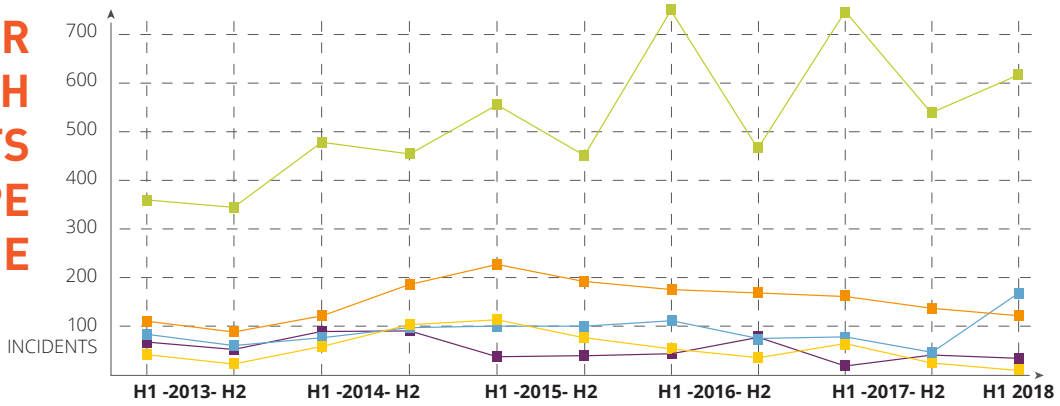




DATA BREACHES BY TYPE

2018 FIRST HALF REVIEW

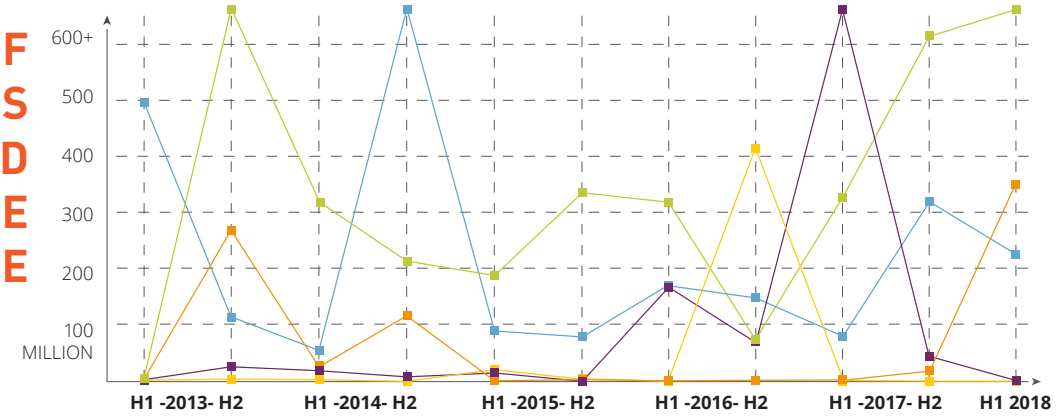
NUMBER OF BREACH INCIDENTS BY TYPE OVER TIME



TYPE OF BREACH	2013		2014		2015		2016		2017		2018
	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1
Identity Theft	369	347	485	455	561	456	774	476	826	541	610
Account Access	80	59	74	97	100	99	109	73	74	59	166
Financial Access	108	85	119	184	224	190	178	176	171	133	123
Nuisance	64	49	87	87	34	37	38	69	21	38	37
Existential Data	38	19	57	101	113	73	64	34	70	27	9
TOTALS	659	559	822	924	1,032	855	1,163	830	1,162	798	945

Source: BREACHLEVELINDEX.COM

NUMBER OF RECORDS BREACHED BY TYPE OVER TIME



TYPE OF BREACH	2013		2014		2015		2016		2017		2018
	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1
Identity Theft	6,152,772	1,183,250,626	320,301,914	215,270,492	188,902,284	337,957,794	318,340,752	79,160,614	323,454,189	621,276,348	3,972,437,893
Financial Access	4,088,747	270,371,346	34,905,015	117,209,547	1,200,098	2,943,207	2,147,030	2,374,097	2,709,295	22,669,150	359,100,353
Account Access	498,231,533	111,457,991	50,941,357	918,530,886	89,681,373	82,191,718	175,606,078	154,392,156	84,045,994	319,077,277	219,940,422
Nuisance	2,664,521	26,159,780	19,539,907	8,421,285	15,032,468	268,354	168,463,495	72,245,752	1,542,034,596	47,990,745	1,694,029
Existential Data	2,060,093	3,529,008	2,963,243	383,174	21,284,889	4,000,389	451,955	415,008,711	425,284	7,586	11
TOTALS	513,197,666	1,594,768,751	428,651,436	2,459,815,384	316,101,112	427,361,462	665,009,310	723,181,330	1,952,669,358	1,011,021,106	4,553,172,708

Source: BREACHLEVELINDEX.COM

COMPARING THE INDUSTRIES

Social Scrapes

From an industry perspective, **social media** giants including Twitter and Facebook witnessed the greatest number of compromised records in H1 2018 at 2,555,000,000. That's a 14,927 percent increase from the previous year. Between 2017 and 2018, the number of incidents involving social media held steady at just six.

There were a few other industries where the number of breached accounts increased by more than a thousand percent:

Industrial saw the highest growth rate amongst all other sectors at 83,787 percent, representing growth from 22,172 to 18,599,592. This data disclosure occurred in just 31 incidents, which was down from 41 a year earlier.

There were just 55 incidents that affected **retail** organizations in H1 2018. This number of security events was 62.5 percent less than the previous year. Even so, the number of breached records increased more than 3,088 percent from 5,839,707 to 186,181,014.

The sum of compromised records involving **professional services** increased 1,061 percent from 9,130 in H1 2017 to 106,001 a year later. During the same time period, the number of incidents in the industry increased by 300 percent to 68 events.

Other sectors experienced more modest growth in either the number of compromised records or security incidents. For instance, while the amount of breached accounts for **government** increased 175.1 percent to 1,212,197,272 in H1 2018, the number of incidents declined 48.3 percent to 61. It was a similar case for **hospitality**, where the number of exposed files grew 272.6 percent to 3,720,296 and the quantity of events fell by 42.3 percent to 15, and for **technology**, where the sum of compromised records went up by 187 percent to 171,467,788 and the total events decreased 56.5 percent to 37.

Meanwhile, **insurance** incidents increased by 36.4 percent from 11 to 15 even though the number of compromised records fell by more than 80 percent to 24,294.

During the same reporting period, there were a few industries that declined in both the number of security incidents and breached records:

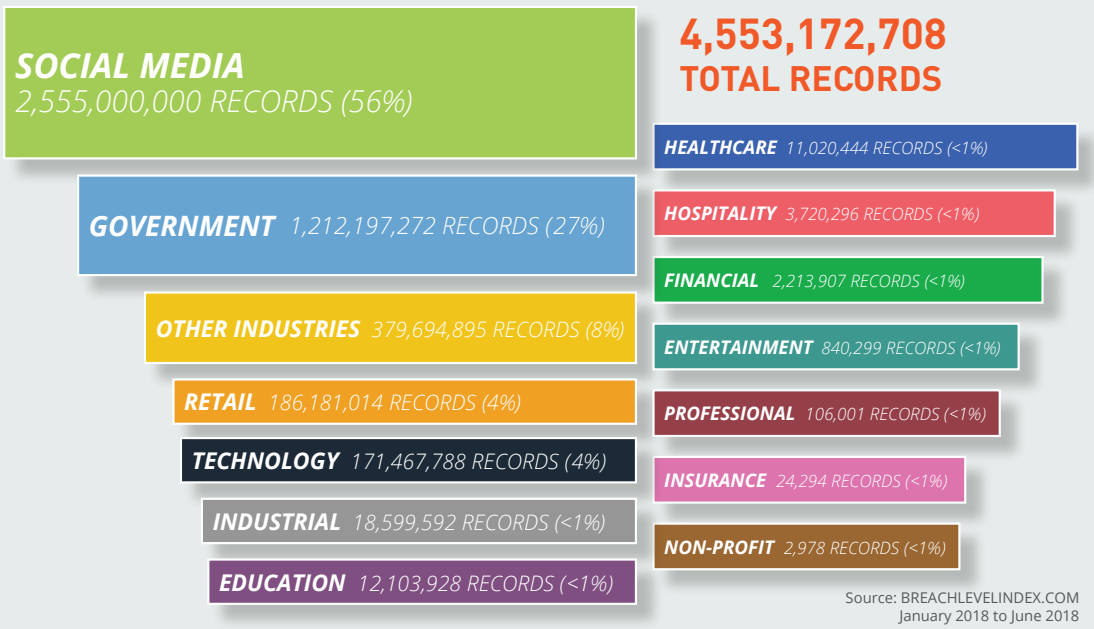
Healthcare companies experienced the greatest amount of security events in H1 2018 amongst all the industries at 256. (Medical organizations were also at the top of the list in the first half of H1 2017, though the number of incidents was higher at 305.) Over the course of that year, the number of disclosed records fell 65.4 percent to 11,020,444. Organizations in **education**, **entertainment**, **financial services** and the **non-profit** sector all saw between 50 percent and 100 percent fewer breached records in H1 2018. The number of incidents for all of those industries also decreased by at least 14 percent and as much as 70 percent.

Those declines weren't random. The decreases observed in healthcare and financial services, for example, could be at least partly attributed to a number of different national regulations that now help regulate health data and financial transactions.

DATA BREACHES BY INDUSTRY 2018

FIRST HALF REVIEW

NUMBER OF RECORDS BREACHED BY INDUSTRY FIRST HALF OF 2018



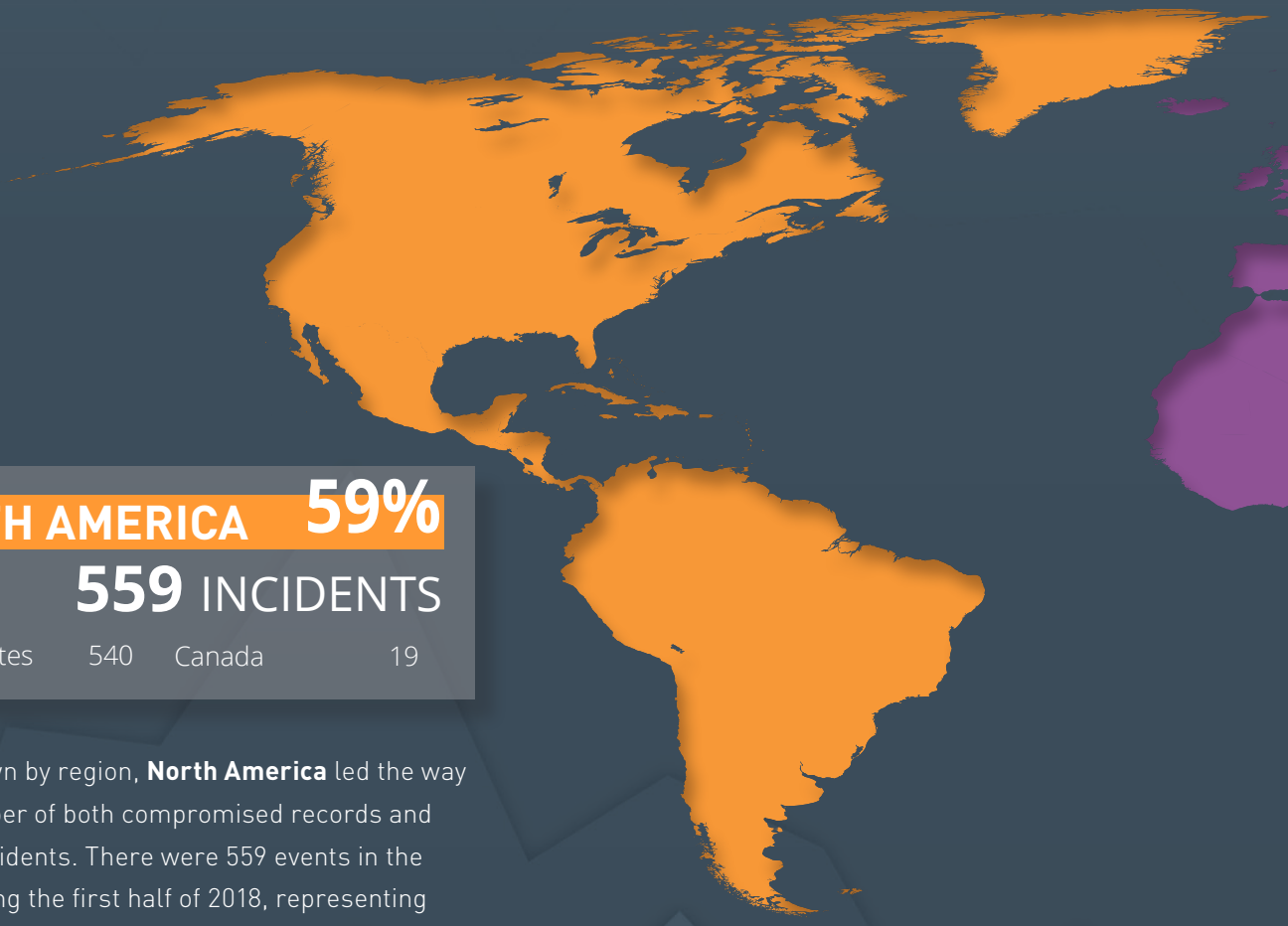
Source: BREACHLEVELINDEX.COM
January 2018 to June 2018

NUMBER OF BREACH INCIDENTS BY INDUSTRY OVER TIME

INDUSTRY	2013		2014		2015		2016		2017		2018
	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1
Healthcare	176	170	242	209	239	215	301	236	305	223	256
Other Industries	152	111	138	137	176	140	116	46	59	27	159
Financial Services	80	85	87	126	154	122	145	97	156	87	134
Education	8	30	86	88	102	64	108	58	136	78	86
Professional Services	-	-	-	1	0	0	0	1	17	88	68
Government	131	65	114	180	161	138	162	127	118	89	61
Retail	56	41	82	115	132	109	122	126	147	75	55
Technology	55	57	73	67	61	63	121	84	85	59	37
Industrial	-	-	-	-	-	-	20	12	41	24	31
Hospitality	1	0	0	1	2	0	15	15	26	15	15
Insurance	-	-	-	-	1	1	9	6	11	14	15
Entertainment	-	-	-	-	3	2	20	10	37	9	11
Non-Profit	-	-	-	-	-	-	17	11	18	7	11
Social Media	-	-	-	1	1	1	1	1	6	3	6
TOTALS	659	559	822	924	1,032	855	1,163	830	1,162	798	945

Source: BREACHLEVELINDEX.COM

A GEOGRAPHICAL VIEW



NORTH AMERICA 59%

559 INCIDENTS

United States 540 Canada 19

Broken down by region, **North America** led the way in the number of both compromised records and security incidents. There were 559 events in the region during the first half of 2018, representing a 45.3 percent decrease over the previous year, but incidents in North America still made up 59.2 percent of the global total. More significantly, the number of breached accounts grew by 98.1 percent from 1,646,281,851 in H1 2017 to 3,262,008,185 a year later. This most recent figure accounted for 71.6 percent of data records compromised worldwide.

In North America, two countries made up the entirety of recorded breaches. The first was the United States at 57.1 percent of the global total of breaches (540 incidents) and 71.5 percent of the worldwide amount of compromised accounts (3,255,712,742 files). The second was Canada, where there were 19 security incidents — two percent of the global average — that resulted in the exposure of 6,295,443 breached records.

By comparison, the whole of **Europe** represented just 3.8 percent of the total number of breaches and 0.5 percent of the global amount of compromised records in H1 2018. This region saw the number of breaches in Ireland grow by a third to four incidents. Over the same time period, the amount of security incidents in Austria, Italy, the Czech Republic, Lithuania and Romania all decreased by 100 percent exactly.

2018
FIRST HALF REVIEW

EUROPE 4%
36 INCIDENTS

United Kingdom	22	Netherlands	1
Ireland	4	Norway	1
France	2	Spain	1
Belgium	1	Sweden	1
Luxembourg	1	Ukraine	1
Malta	1		

ASIA / PACIFIC 36%
339 INCIDENTS

Australia	308	China	2
India	12	New Zealand	2
Japan	5	Philippines	1
Hong Kong	4	South Korea	1
Malaysia	3	Tailand	1

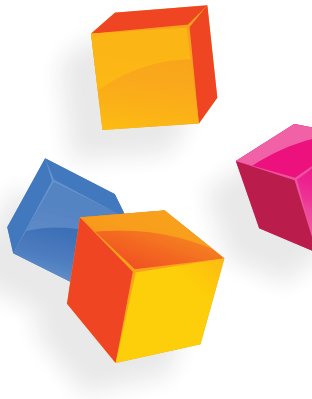
MIDDLE EAST / AFRICA 1%
10 INCIDENTS

GLOBAL
1 INCIDENT

The **Middle East** saw impressive growth rates in both the amount of security incidents (133.3 percent) and the number of compromised files (2,910 percent). Even so, these surges brought the region's global representation in both events and breached records to just 0.7 percent. **Africa** made up an even smaller global representation at 0.3 percent of the security incidents and 0.02 percent of exposed accounts.

The same cannot be said about the **Asia / Pacific** region, which accounted for 35.9 percent of the global number of security events and 27.2 percent of compromised records. Australia in particular saw the totals of its data breaches and compromised records both increase by more than 1,000 percent. Other countries in the region including India, New Zealand, Japan, Hong Kong, Malaysia and the Philippines also saw significant growth in one of their totals.

SECURITY LESSONS FROM 2018



In the first half of 2018, data breaches declined by 18.7 percent from the previous year to 945 security incidents. Yet the findings of **the Breach Level Index for H1 2018 suggest that data breaches continue to get faster and bigger.** Despite a decrease in security incidents, the first half of 2018 witnessed the numbers of records compromised every day, hour, minute and second more than double over the previous year's figures. Meanwhile, the total amount of breached records recorded in H1 2018 increased by 133 percent, with the number of breaches affecting more than one million accounts also becoming more numerous compared to H1 2017.

The data collected by Gemalto's BLI highlights three trends that organizations should consider moving forward. These are as follows:

Spend your security dollars wisely.

According to *Gartner*, worldwide spending on information security products and services will increase 12.4 percent and reach more than $114 billion in 2018. That number is expected to grow an additional 8.7 percent to $124 billion by 2019. But even as security spending continues to increase, so too do the number of stolen or compromised data records. This means that organizations are continuing to spend more on the same conventional technologies that monitor and protect the perimeter. Since the traditional perimeter of the enterprise has been blown up by the cloud, the new perimeter is the data itself and the users accessing that data. Mindsets need to change to adapt to this reality, and IT professionals need to accept that breaches will occur and attach security directly to the data itself and the users.

Funding will have a limited impact on digital crime.

Observations of the current digital crime landscape present a dismal picture of the effectiveness of the security investments mentioned above. For example, *Cybersecurity Ventures* anticipates that the costs associated with digital crime will exceed $6 trillion by 2021, thereby doubling the losses reported in 2015. *Cisco's* expectation is that these costs will at least in part include attacks against IP networked devices, of which there will be 26 billion in 2020 (up from 16.3 billion in 2015).

We are the problem.

Human errors and poor security practices continue to be a major source of data breaches. Mobile security researchers observed this trend in action when they found that the *Firebase databases* for thousands of Android and iOS apps were unprotected and had thereby exposed approximately 100 million data records. To counter these types of incidents, organizations need to bolster their internal security by training their employees and adopting the following security measures:

Encryption. Encryption can render sensitive data unreadable to attackers but only when it's enabled. This security measure was used in only 21 (2.2%) of the security incidents reported in H1 2018. Those breaches resulted in protecting only 42,740,464 data records (less than 1%).

Access Management, including Multi-Factor Authentication. This security control can help protect users even if their account credentials or devices have been stolen. That's why Twitter recommended that users implement some form of two-factor authentication on their accounts after discovering the glitch involving its internal password logs. Along with MFA, it's important that organizations have an access management program in place to limit data access to the necessary people. Those individuals who do have access should be properly trained in order to minimize the threat of a data breach.

BREACH PREPAREDNESS 2018

FIRST HALF REVIEW

Start by Staying Secure in the Cloud

Organizations that use Amazon Web Services S3 buckets and other cloud-based assets to store their data can't assume that they're automatically protected against a security incident. They need to remember that there's such a thing as "security in the cloud," which means they have a responsibility to protect their cloud-based data by **using encryption and other security practices, managing privileged access and maintaining compliance.**

Regulations and Reporting Data Breaches

Data breach reports are increasing under the new data protection regulations. Going forward, it's likely that more data breach notifications will continue to occur under Australia's NDB scheme as well as the European Union's GDPR before leveling off as companies increasingly achieve compliance. Security best practices like **securely managing cryptographic keys and controlling data access** can help get companies to this level of compliance early.

Steps Towards Securing the Breach

With the two other parting thoughts serving as guidance, there are three steps that every company should take to mitigate the overall cost and consequences of a security breach: **encrypt all sensitive data at rest and in motion, securely store and manage all of your encryption keys and control access and authentication of users.** By implementing each of these three steps, companies can effectively prepare for a breach and avoid falling victim to one.

WHAT'S YOUR SCORE?

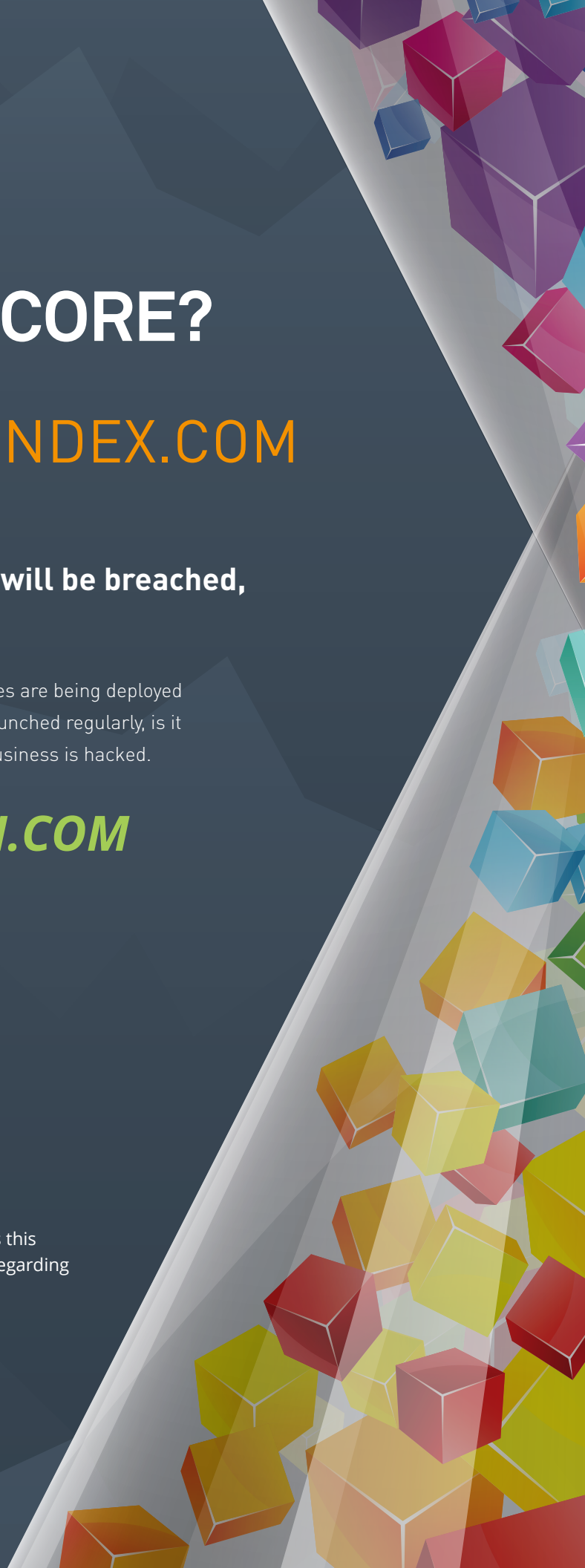
FIND OUT AT

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 office locations and contact information, visit safenet.gemalto.com.