2015

First Half Review

Findings from the

BREACH LEVEL INDEX

POWERED BY

gemalto

security to be free

BREACH LEVEL INDEX

THE NUMBERS

> *More and more organizations are accepting the fact that, despite their best efforts, security breaches are unavoidable.*

RECORDS BREACHED IN FIRST HALF OF 2015

245,919,393

NUMBER OF BREACH INCIDENTS

888

TOP 10 BREACHES PERCENTAGE OF TOTAL RECORDS

82%

PERCENTAGE OF BREACHES WHERE NUMBER OF COMPROMISED RECORDS WAS UNKNOWN

50%

DATA RECORDS WERE LOST OR STOLEN WITH THE FOLLOWING FREQUENCY

- EVERY DAY 1,358,671
- EVERY HOUR 56,611
- EVERY MINUTE 943
- EVERY SECOND 16

INTRODUCTION

2015
FIRST HALF REVIEW

The first six months of 2015 demonstrated that hackers continue to get past conventional perimeter security with relative ease, targeting nearly every industry and executing several high profile data breaches that scored tens of millions of data records each. And, while Identity Theft remains one of the leading types of data breaches, the first half of 2015 has shown a shift in attack targets. For example, data records stolen from state-sponsored attacks rose dramatically compared to previous years and healthcare and government overtook retail as the major sectors under siege with the number of compromised data records.

The 2015 First Half Review Key Findings

According to the latest findings of the **Breach Level Index** produced by digital security company **Gemalto**, 888 data breaches occurred in the first half of 2015, compromising 245.9 million records worldwide. The number of breaches was relatively flat compared with the last six months of 2014 (892) but increased by 10% compared to the 803 data breaches in first half of 2014.

A more dramatic decline was in the number of breached records which fell by 40% from the 414.8 million records breached in the first half of last year. There was an even greater drop (61%) in the number of breached records compared with the second half of 2014, which saw a total of 626.4 million records exposed.

One notable statistic is that for nearly 50% of the reported first half 2015 data breaches, the total number of data records that were compromised is unknown.

Large, headline-grabbing data breaches continue to expose massive amounts of stolen records. The biggest breach in the first half of this year, which scored a 10 on the Breach Level Index magnitude scale, was an identity theft attack on Anthem Insurance that exposed 78.8 million records. That attack represented one third (32%) of the total records exposed in the first half of 2015, and was highly publicized in part because it represented the first major state-sponsored cyber-attack of several that occured in 2015.

Other notable breaches in the analysis period included a breach of 21 million records at the U.S. Office of Personnel Management, with a Breach Level Index score of 9.7; a 50 million record breach at Turkey's General Directorate of Population and Citizenship Affairs with a score of 9.3; and a 20 million record breach at Russia's Topface with a score of 9.2. The top 10 breaches accounted for 82% of all compromised records in the first half of the year.

To create the Breach Level Index, Gemalto gathers extensive information about data breaches worldwide, using sources including Internet searches, news articles and analyses, and other resources.

The data is aggregated into the Index where it is analyzed according to the number of breaches and data records lost and categorized by industry, type of breach, source of breach, and tallied by country or region.

NOTABLE DATA BREACHES

Anthem Insurance
Score: **10.0**
Records: **78,800,000**

The U.S. based health insurance provider was hit with a state-sponsored, identity theft breach in February 2015. Criminal hackers broke into the firm's servers and stole 78.8 million records that contain personally identifiable information. According to Anthem, the data breach extended into multiple brands that the company uses to market its healthcare plans including: Anthem Blue Cross, Anthem Blue Cross and Blue Shield, Blue Cross and Blue Shield of Georgia, Empire Blue Cross and Blue Shield, Amerigroup, Caremore, and UniCare.

General Directorate of Population and Citizenship Affairs
Score: **9.9**
Records: **50,000,000**

The Turkish government agency suffered an identity theft attack from a malicious outsider that resulted in the theft of 50 million records. According to the Presidency's State Audit Institution, the servers of the administration's website were easily breached and information about citizens was stolen.

U.S. Office of Personnel Management (OPM)
Score: **9.6**
Records: **21,000,000**

In June 2015, the OPM was the target of a data breach that involved 21 million records. This was a state-sponsored identity theft attack which has been described by federal officials as one of the largest breaches of government data in the history of the U.S. Information targeted in the breach included personally identifiable information such as Social Security numbers, names, dates and places of birth, and addresses.

Topface
Score: **9.2**
Records: **20,000,000**

This Russia-based online dating service experienced an account access breach by a malicious outsider that resulted in the theft of 20 million records. According to a Bloomberg report, the stolen information included the user names and e-mail addresses of 20 million visitors to the site.

Gaana.com / Times Internet
Score: **8.9**
Records: **10,000,000**

One of India's most popular music streaming services was hit with an identity theft attack by a malicious outsider that affected 10 million records. According to The Hacker News, the records stolen included user names, email addresses, passwords, birthdates, and other personal information.

TOP SCORING BREACHES

2015
FIRST HALF REVIEW

The Breach Level Index score, which rates the severity of a data breach, is based on factors such as total number of records breached, type of data in the records, source of the breach, and how the information was used. 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 scale shows that not all data breaches have the same impact on organizations.

ORGANIZATION	RECORDS	TYPE	INDUSTRY	SCORE
ANTHEM INSURANCE COMPANIES (ANTHEM BLUE CROSS) (U.S.)	78,800,000	IDENTITY THEFT	HEALTHCARE	10.0
GENERAL DIRECTORATE OF POPULATION AND CITIZENSHIP AFFAIRS/THE GENERAL DIRECTORATE OF LAND REGISTRY AND CADASTER (TURKEY)	50,000,000	IDENTITY THEFT	GOVERNMENT	9.9
U.S. OFFICE OF PERSONNEL MANAGEMENT (U.S.)	21,000,000	IDENTITY THEFT	GOVERNMENT	9.6
TOPFACE (RUSSIA)	20,000,000	ACCOUNT ACCESS	TECHNOLOGY	9.2
GAANA.COM / TIMES INTERNET (PAKISTAN)	10,000,000	IDENTITY THEFT	RETAIL	8.9
RAKUTEN AND LINE CORP (JAPAN)	7,850,000	ACCOUNT ACCESS	RETAIL	8.8
TALKTALK (U.K.)	4,000,000	IDENTITY THEFT	OTHER	8.8
MEDICAL INFORMATICS ENGINEERING (U.S.)	3,900,000	IDENTITY THEFT	HEALTHCARE	8.8
ADULT FRIENDFINDER (U.S.)	3,867,997	EXISTENTIAL DATA	OTHER	8.6
REGISTER.COM (U.S.)	1,400,000	EXISTENTIAL DATA	TECHNOLOGY	8.5
SAUDI ARABIA GOVERNMENT (SAUDI ARABIA)	1,000,000	EXISTENTIAL DATA	GOVERNMENT	8.4

DATA BREACHES BY SOURCE

The leading source of data breaches in the first half of 2015 continues to be **malicious outsiders**, who are responsible for 546 of the breaches in this period and comprise 61.5% of the total. The share of attacks attributed to outsiders has risen steadily since the first half of 2013 when it accounted for only 52%.

Accidental loss is the next highest source of data breaches. At 197, **accidental loss** accounts for 22.2% of all data breaches in the first half of 2015. Rounding out the top five source types are **malicious insiders** (107 breaches for 12.0%), **hacktivists** (19 breaches for 2.5%), and **state sponsored** (17 breaches for 2.2%).

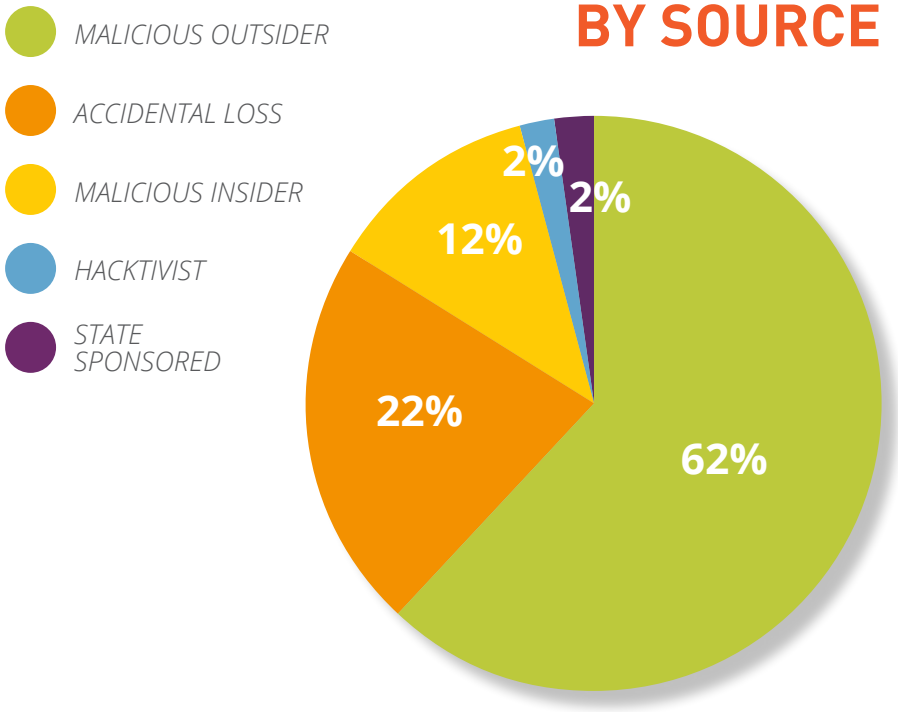
Compromised Data Records

In terms of compromised data records, **malicious outsiders** took the top spot with 114.5 million stolen. This accounted for nearly half of all the records exposed in breaches during the period (46.6%). It's notable that the share was down considerably from first half of 2013 (93.2%), the second half of 2013 (96.3%), and the first half of 2014 (71.8%). It was similar to the 42% share in the second half of last year, which may indicate that records lost due to breaches by malicious outsiders have leveled off.

The next highest source of data records lost was **state-sponsored** attacks with 101.5 million (41.3%). That was a significant increase from any previous period since 2013. For example, in 2013 and 2014, the amount of data records affected by state-sponsored breaches was negligible and garnered a share of just 1.1% of all records in the second half of 2014.

Other sources of records theft in first half of 2015 were **accidental loss** (28.6 million for 11.6%), **malicious insiders** (784,000 for 0.3%), and **hacktivists** (562,000 for 0.2%). The number of records affected by accidental loss dropped dramatically from the second half of 2014, when it was 305.2 million for 48.7%. Similarly, the amount of records lost because of malicious insiders has decreased sharply from 106.2 million (25.6%) in the first half of 2014 and 52.9 million (8.5%) in the second half of that year.

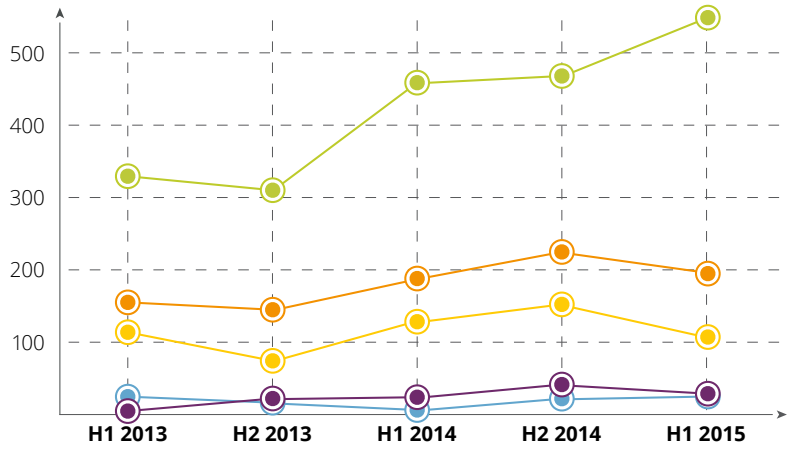
NUMBER OF BREACH INCIDENTS BY SOURCE



DATA BREACHES BY SOURCE OVER TIME

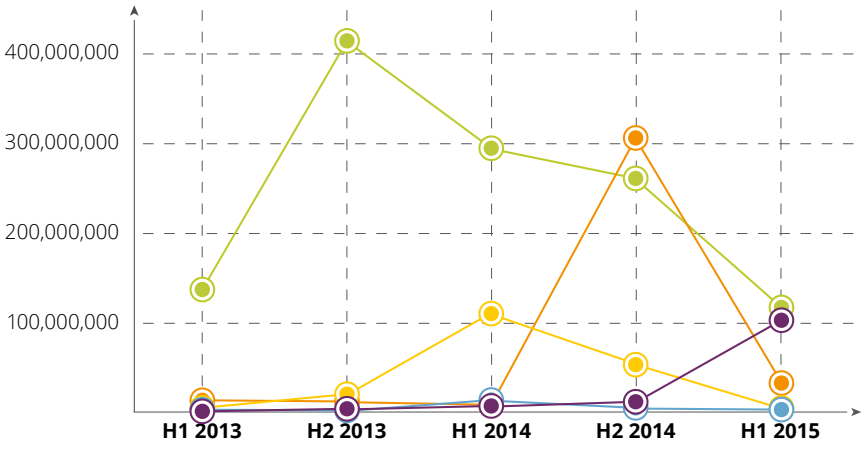
2015
FIRST HALF REVIEW

NUMBER OF BREACH INCIDENTS BY SOURCE OVER TIME



SOURCE	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015
Malicious Outsider	335	314	465	470	546
Accidental Loss	159	140	189	216	197
Malicious Insider	114	78	125	153	107
Hacktivist	21	8	4	15	19
State Sponsored	3	10	20	40	17

NUMBER OF RECORDS BREACHED BY SOURCE OVER TIME



SOURCE	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015
Malicious Outsider	142,693,717	409,067,412	297,681,964	263,311,253	114,520,847
Accidental Loss	8,482,892	6,140,675	3,425,588	305,285,159	28,568,633
Malicious Insider	1,149,769	9,200,723	106,190,172	52,947,689	784,329
Hacktivist	777,216	98,730	7,000,096	1,182,005	561,918
State Sponsored	38	165,015	3,016,499	6,912,064	102,883,225

DATA BREACHES BY TYPE

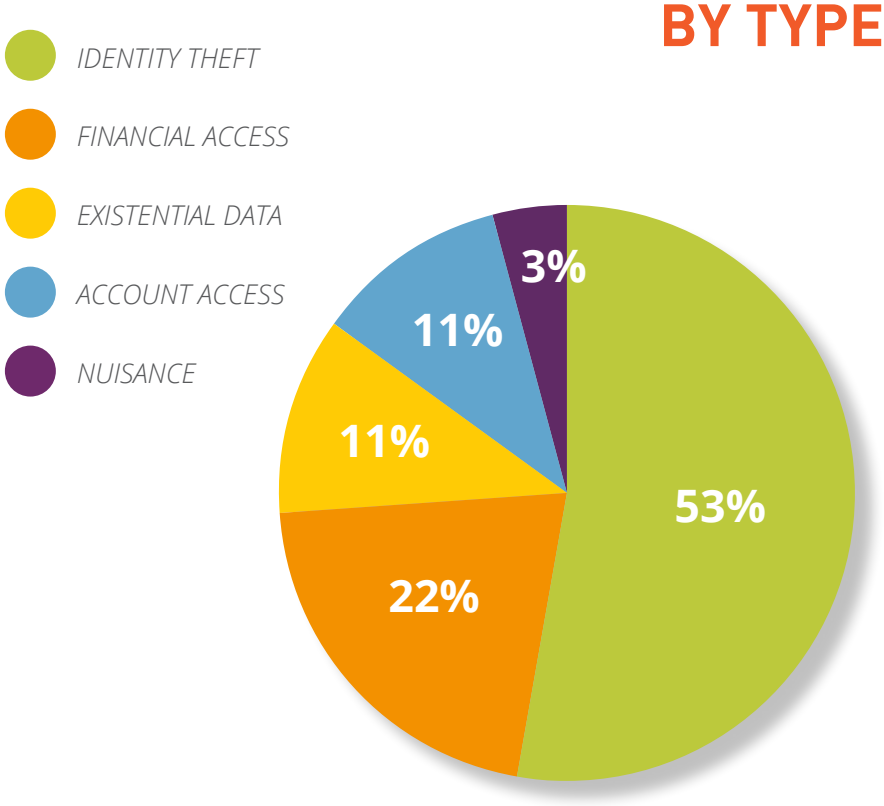
During the first half of 2015, attackers used a variety of techniques against organizations to acquire personal identities, financial data, or access to account information.

The leading type of data breach in the first half of 2015 was **identity theft** as the cause of 472 data breaches, accounting for more than half (53.2%) of first half 2015 attacks and nearly three-quarters (74.9%) of compromised data records. Five of the top 10 breaches in the first half 2015, including the top three, were identity theft breaches.

The next most common type of data breach was **financial access** to data. Responsible for 197 breaches in the first half, financial access accounts for 22.2% of the total but only about 1% of compromised data records. Other data breach types include **existential data** (96 breaches, 10.8%), **account access** (93 breaches, 10.5%) and **nuisance** (30 breaches, 3.4%).

The frequency of these attack types in the first half of the year is largely in line with all of 2014 with some minor fluctuations in the percentages.

NUMBER OF BREACH INCIDENTS BY TYPE



Compromised Data Records

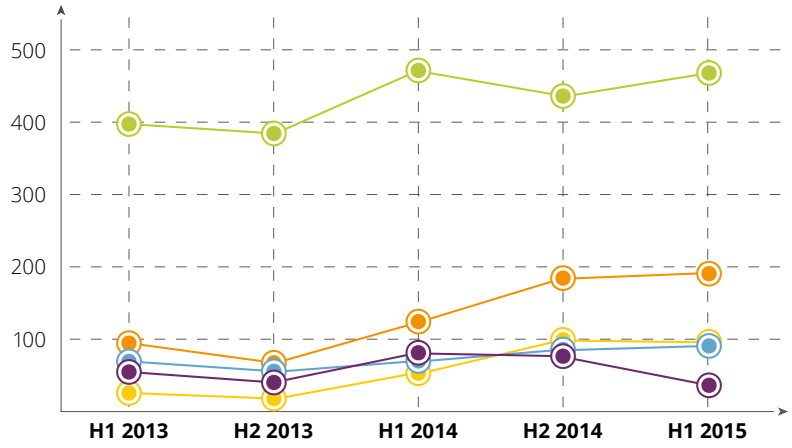
Concerning compromised data records, **identity theft** also was the leading cause of data records exposure in the first half of 2015 with 185.7 million records, or about three quarters of all records (74.9%), exposed in the first half. Next was **account access** (34.3 million for 13.9%), followed by **nuisance** (15 million for 6.1%), **existential data** (8.8 million for 3.6%) and **financial access** (2 million for 0.8%).

Perhaps the most notable changes compared with the second half of 2014 were that the share of data records attributed to identity theft that were stolen rose from 30.2%, and stolen data records attributed to account access dropped from 50.2%.

DATA BREACHES BY TYPE OVER TIME

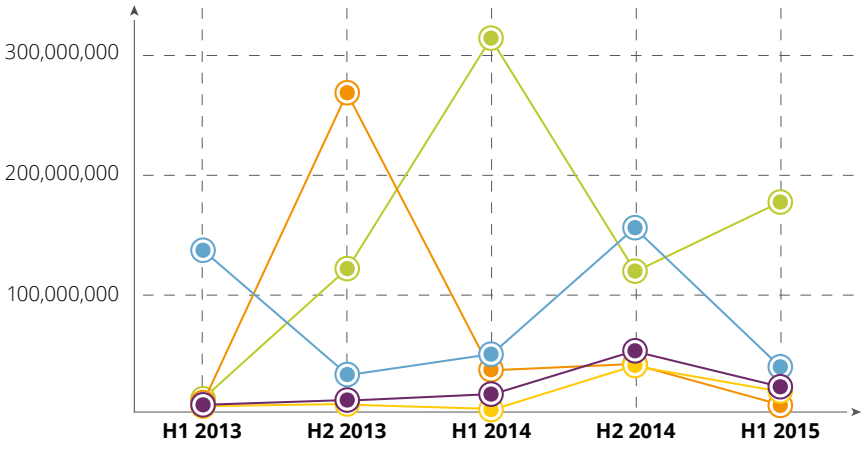
2015
FIRST HALF REVIEW

NUMBER OF BREACH INCIDENTS BY TYPE OVER TIME



TYPE OF BREACH	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015
Identity Theft	396	382	474	443	472
Financial Access	97	71	119	183	197
Existential Data	25	13	54	98	96
Account Access	76	52	74	92	93
Nuisance	55	35	86	81	30

NUMBER OF RECORDS BREACHED BY TYPE OVER TIME



TYPE OF BREACH	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015
Identity Theft	6,436,318	121,624,113	316,003,444	115,316,845	185,717,096
Financial Access	4,060,027	270,264,132	34,905,015	35,876,605	2,071,434
Existential Data	1,818,066	3,323,008	555,843	35,573,128	8,784,671
Account Access	138,226,695	23,375,563	50,911,957	156,442,510	34,315,208
Nuisance	2,635,306	6,090,484	14,939,907	50,882,682	15,030,984

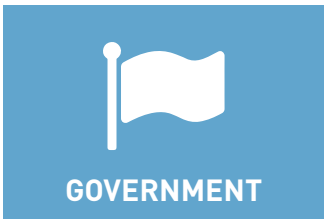
HOW THE INDUSTRIES COMPARE

The **healthcare** industry historically has had the highest number of data breaches and that was no different in the first half of 2015. The sector experienced

187

breaches, accounting for 21.1% of the total. That's actually down from recent half-year periods, both in the number of breaches and in the share of breaches among industries.

The next industry with the highest number of breaches was **financial services**, with 143 breaches in the first half, for a 16.1% share of the total. Closely following financial services was **government**, which



saw 140 breaches in the first half, for a 15.8% share of the total. Following these were **retail** (115 for 13.0%), **education** (94 for 10.6%), and **technology** (46 for 5.2%). The remaining 163 data breaches in the first half were divided up among several **other industries**, and accounted for 18.4% of the first half total.

As for the number of data records lost by industry, **healthcare** took the top spot with

84.4 million

records or 34% of the total. **Government** accounted for 77.2 million records lost with 31.4%.

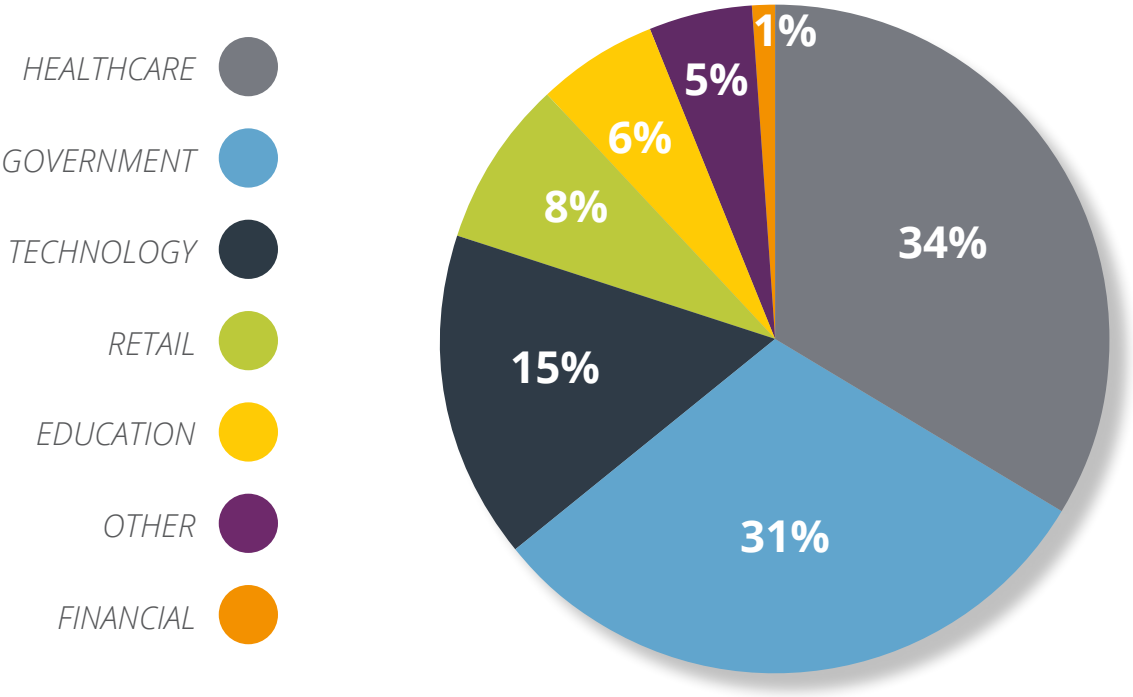
This represents a dramatic shift from the past few years when both healthcare and government had relatively small numbers of records involved in data breaches. For example, in the second half of 2014, healthcare accounted for only 5.2% of stolen records and government accounted for only 2.8%. In previous periods, the number of records involved in data breaches was mostly in retail and financial services industries.

Following healthcare and government in the number of records for the first half of 2015 were **technology** (37.5 million for 15.2%), **retail** (18.6 million for 7.6%), **education** (15.7 million for 6.4%), and **financial services** (683,133 for 0.3%).

HOW THE INDUSTRIES COMPARE

2015
FIRST HALF REVIEW

NUMBER OF RECORDS BREACHED BY INDUSTRY

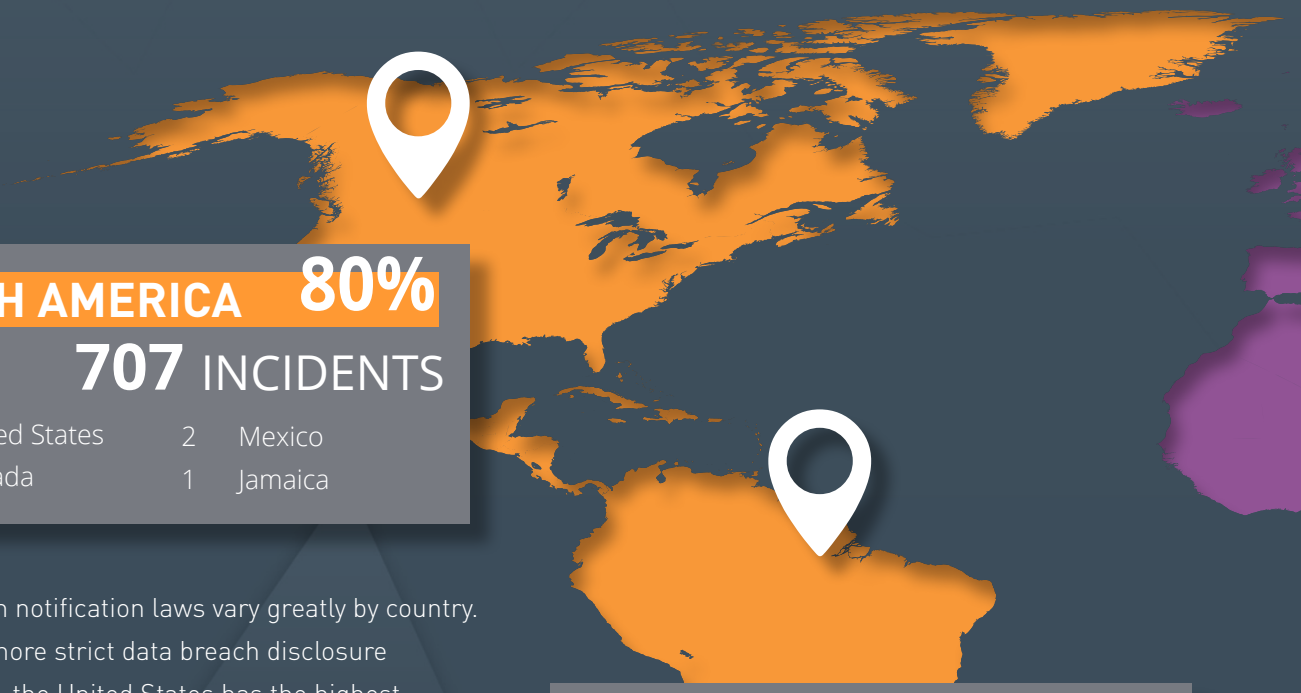


NUMBER OF BREACH INCIDENTS BY INDUSTRY OVER TIME

INDUSTRY	H1 2013	H2 2013	H1 2014	H2 2014	H1 2015
Healthcare	172	168	236	200	186
Financial Services	79	87	85	125	143
Government	128	65	108	182	142
Retail	58	42	83	112	115
Education	7	26	88	84	94
Technology	56	54	72	65	47
Other Industries	151	113	142	131	161

BREACH LEVEL INDEX

THE GEOGRAPHIC VIEW



NORTH AMERICA 80%

707 INCIDENTS

671	United States	2	Mexico
33	Canada	1	Jamaica

SOUTH AMERICA <1%

4 INCIDENTS

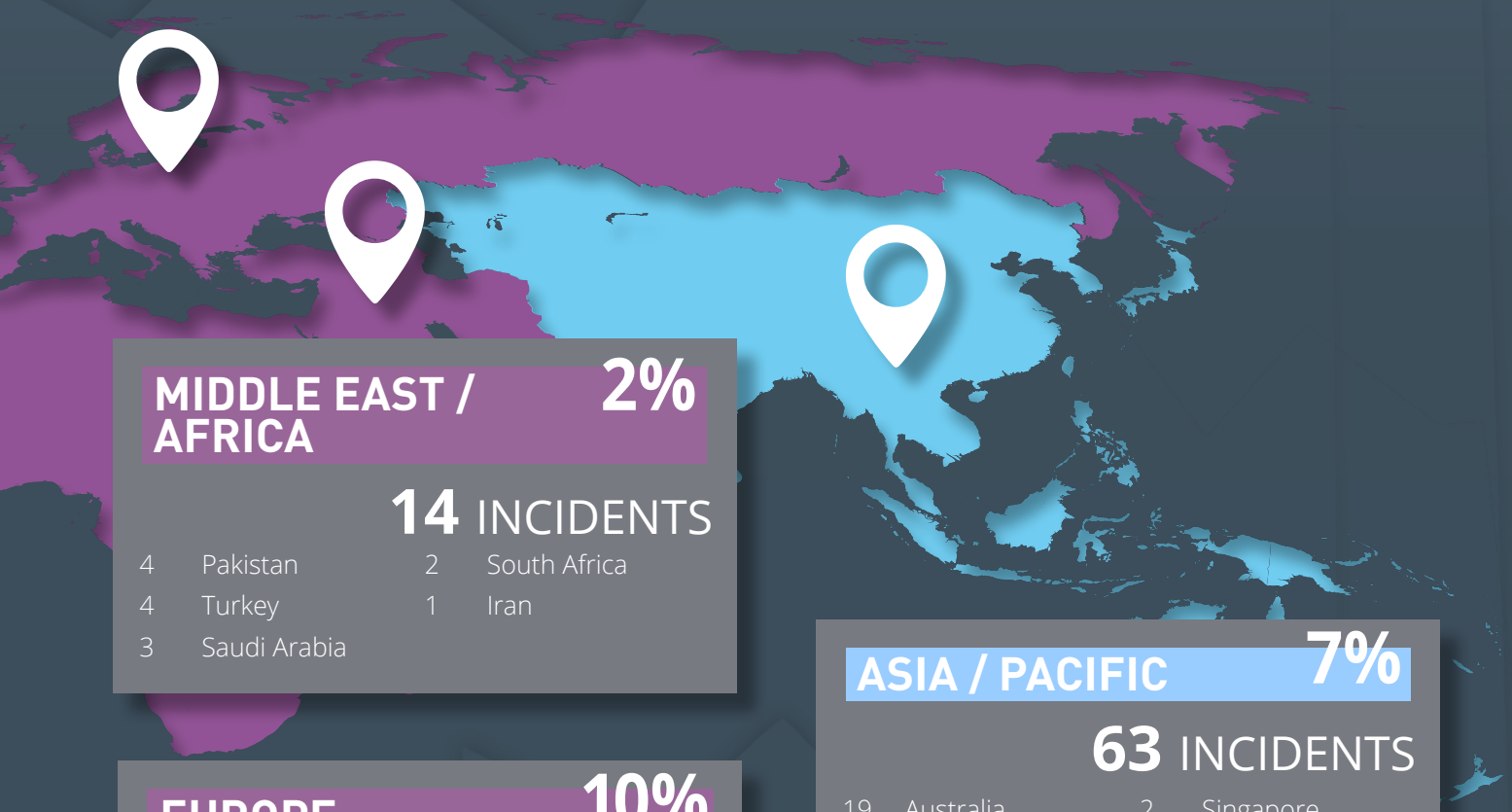
2	Chile
1	Brazil
1	Columbia

Data breach notification laws vary greatly by country. Due to its more strict data breach disclosure regulations, the United States has the highest number of reported data breaches. For the 28 European Union member countries, they will likely see an increase in reported data breaches once the European Commission adopts General Data Protection Regulation sometime in 2016.

With 707 reported breaches (79.6% of the total), North America once again led all regions in the number of data breaches in the first half of 2015. This was an increase of 11.4% compared to the first half of last year when the region saw 633 breaches (78.8%). Europe was a distant second, with 94 breaches (10.6%), followed by Asia Pacific with 63 (7.1%), the Middle East / Africa with 14 (1.6%), and South America with 4 (0.4%). Those figures were not much different from the findings in the first half of 2014.

North America also was the top region for records exposed, with 121.2 million (49.3%). That compares with 112 million (27%) in the first half of 2014. Next highest in records exposed was the Middle East, with 76.5 million for 31.1%. Europe had 36.6 million compromised data records (14.9%), Asia Pacific had 11.5 million (4.7%), and South America with just 4,360 records exposed for less than 1%. The most dramatic changes in records exposed from the first half of 2014 were a significant increase for the Middle East and significant drop for Asia Pacific.

2015
FIRST HALF REVIEW



MIDDLE EAST / AFRICA — 2%

14 INCIDENTS

4	Pakistan	2	South Africa
4	Turkey	1	Iran
3	Saudi Arabia		

EUROPE — 10%

94 INCIDENTS

63	United Kingdom	2	Russia
8	Germany	2	Switzerland
6	Netherlands	1	Belgium
4	France	1	Europe
2	Austria	1	Finland
2	Italy	1	Ireland

ASIA / PACIFIC — 7%

63 INCIDENTS

19	Australia	2	Singapore
9	India	2	Taiwan
9	Japan	2	Thailand
8	New Zealand	2	Vietnam
6	China	1	Kazakhstan
2	Hong Kong	1	Malaysia

In terms of individual countries, the United States had the most data breaches in the first half of 2015 (671 for 75.6%), followed by the United Kingdom (63 for 7.1%) and Canada (33 for 3.7%). The U.S. also had the most records involved in breaches with 120.9 million which accounted for 48.8% of the total.

Turkey had 65 million (6.2%) records exposed and the United Kingdom with 8.3 million records exposed for 3.4% of the total.

A NEW MINDSET FOR DATA SECURITY

Breach Prevention Alone Has Failed

The First Half 2015 Breach Level Index from Gemalto shows that data breaches are very much a growing threat for organizations. The number of records compromised is remarkable considering the lengths many organizations go to in order to protect their data.

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. Enterprises are not investing in security based on reality as it is; they're investing in security based on reality as it was: a bygone era where hackers were glory-seeking vandals, sensitive data was centralized, and the edge of the enterprise was a desktop PC in a known location. And, back then, in that reality, network firewalls and other network perimeter "breach-prevention" technologies were good enough. 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.

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** against data breaches in the future.

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. Alarmingly, market trends show that the lion's share of organizations have no plans to change this approach. According to research firm IDC, of the $32.6 billion enterprises spent on security technology in 2014, 62% ($20.2 billion) was invested in network and perimeter security.

A NEW MINDSET FOR DATA SECURITY

2015 FIRST HALF REVIEW

From Breach Prevention to Breach Acceptance

The Breach Level Index indicates that data breaches have been increasing in frequency and size over the last couple of years. So, by definition, breach prevention is an irrelevant strategy for keeping out cybercriminals. In addition, every organization already has potential adversaries inside the perimeter. Disregarding these internal threats not only invites blatant misuse but also fails to protect against accidental carelessness. Even non-malicious behaviors such as: bringing work home via personal email accounts, lost devices, storing data on USB drives, and vendors unknowingly sharing network log-in credentials and passwords are a few examples of how easy it is to innocently leak sensitive data.

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. Securing the data is a challenging proposition in a world where cloud, virtualization, and mobile devices are causing an exponential increase in the attack surface. 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.

From Breach Acceptance 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. **Control access and authentication of users. Encrypt all sensitive data** at rest and in motion, and securely **store and manage all of your encryption keys**. By implementing each of these three steps into your IT infrastructure, companies can effectively prepare for a breach and avoid falling victim to one.

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:

www.securethebreach.com

What's Your Score? Find Out At

BREACHLEVELINDEX.COM

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

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