BREACH LEVEL INDEX

SECOND QUARTER RECAP
2014 (April - June)

RECORDS BREACHED APRIL - JUNE

175,655,228

TOP SCORING BREACHES THIS QUARTER

| ORGANIZATION	RECORDS	TYPE	INDUSTRY	SCORE
eBay (United States)	145,000,000	Identity Theft	Retail	**10.0**
City of Verden (Germany)	18,000,000	Financial Access	Government	**9.3**
Bulgaria Citizens (Bulgaria)	2,832,312	Identity Theft	Other	**8.7**
AOL (United States)	2,000,000	Identity Theft	Technology	**8.5**
Montana Dept. PH & HS (United States)	1,300,000	Identity Theft	Government	**8.3**
French Telecoms Group Orange (France)	1,300,000	Identity Theft	Other	**8.3**
Mumsnet Limited (United Kingdom)	1,500,000	Financial Access	Other	**8.3**
Domino's Pizza (France/Belgium)	650,000	Identity Theft	Retail	**8.0**
Harley Medical Group (United Kingdom)	500,000	Identity Theft	Healthcare	**7.9**
Affinity Gaming (United States)	300,000	Financial Access	Other	**7.6**

WHAT THE PAST QUARTER REVEALED

According to publicly available information collected in the Breach Level Index, there were 237 data breaches and more than 175 million data records lost or stolen between April and June of 2014. Encryption was used in only 10 of the 237 reported data breaches. Of those, only two, or less than 1%, were "secure breaches" where strong encryption, key management or authentication solutions rendered the data useless.

On average in Q2 2014, data records were lost or stolen with the following frequency:

| Every DAY	Every HOUR	Every MINUTE	Every SECOND
1,951,724	81,321	1,355	23

TOP BREACH RECORDS BY SOURCE

- Malicious outsider (56%)
- Accidental loss (29%)
- Malicious insider (12%)
- State sponsored (<2%)
- Hacktivist (<1%)
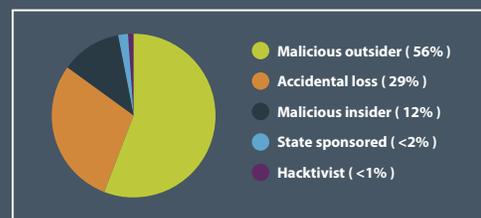
Malicious outsiders claimed the top spot for data breaches in the second quarter of 2014, accounting for 56% of all data breaches. This was followed by accidental loss (29%), malicious insiders (12%), state-sponsored (2%) and hacktivists (<1%). Identity theft was the leading type of data breach representing 58% of all incidents and 88% of records stolen.

TOP DATA BREACHES BY INDUSTRY

- Retail (83%)
- Government (11%)
- Other (4%)
- Technology (<2%)
- Healthcare (<1%)
- Education (<1%)
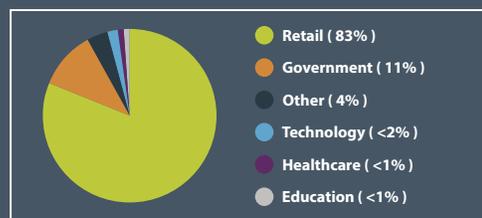
The Retail sector led all industries in terms of records stolen with 145 million, accounting for 83%. eBay's breach of personally identifiable information (name, email, phone number, address and date of birth) was the largest retail breach of the quarter with 145 million records lost. Government represented 11% of the records stolen. Most specifically the Department of Veteran's Administration has had the most breach incidents of any government agency with three separate incidents each accounting for the loss of over 1,000 records. The other five industries (education, government, financial, technology and all others) lost minimal numbers of records totaling only 6 percent.

BREACH LEVEL INDEX

" **MOVE FROM BREACH PREVENTION TO BREACH ACCEPTANCE** "
Focus on the data itself.

SECOND QUARTER RECAP 2014

COUNTRY & REGIONAL PERSPECTIVES

Three of the top five breaches in the world occurred in the United States, a total of 175 incidents, and a loss of 150 million records across a range of industries in the second quarter of 2014. This represents 74% of the total number of reported breached records worldwide and 85% of all the records lost. Europe followed with 25 million or 14% of records lost, while Asia-Pacific, the Middle East and Africa accounted for less than 1% of all records lost. This may be due to strict laws in the U. S. for breach reporting compared to other countries.

TOP ORGANIZATION BREACHES

eBay had the largest data breach in the retail industry in the second quarter of 2014. Attackers compromised employees' log-in credentials through social engineering to gain access to the company's network and compromised a database that contained customer names, encrypted passwords, email addresses, physical addresses, phone numbers and dates of birth. The breach allowed access to 145 million records. Risk Score for this incident is 10.0, since the number of records was so high and the data accessed was critical personal information.

10.0
Risk Score

The **City of Verden** hack became the largest ever data breach in the history of Germany. The usernames and passwords of 18 million email accounts were stolen and compromised by hackers. This Breach Level Index Risk Score is 9.3 due to the amount of records and the personal information that was accessed.

9.3
Risk Score

Hackers were able to steal the email addresses, postal addresses, address books, encrypted passwords and the encrypted answers to security questions of 2 million **AOL** users. This Breach Level Index Risk Score comes in at 8.5 due to the amount of records and the personal information that was accessed.

8.5
Risk Score

A server at **Montana Department of Public Health and Human Services** was hacked by a malicious outsider. The server held the names, addresses, dates of birth and Social Security Numbers of approximately 1.3 million people. Risk Score is 8.3 due to the amount of records and the personal information that was accessed.

8.3
Risk Score

Malicious outsiders breached vulnerable servers belonging to **Domino's Pizza France & Belgium**, stealing the sensitive information of nearly 600,000 customers. The stolen information is said to contain customers' full names, addresses, phone numbers, email addresses, passwords, delivery instructions, and favorite pizza toppings. Risk Score totals 8.0 from the records and information accessed.

8.0
Risk Score

NOT ALL BREACHES ARE CREATED EQUAL

While one industry may lead all others in terms of the number data breaches, it does not always mean that that industry will claim the top spot in terms of data records stolen.
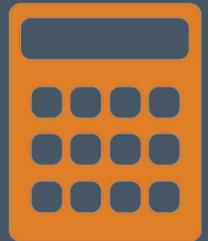
For data breach incidents, the Healthcare industry had the most incidents for the second consecutive quarter with 54 incidents or 23% of total incidents. However, the Healthcare industry had the least amount of records accessed, less than 1% of the total, meaning that the breaches that do occur in the Healthcare industry are "secure" or are keeping attackers from accessing information.

In the Financial Services sector, data breaches decreased significantly from the first quarter, down from 56 percent to less than one percent of records stolen in the second quarter. The financial sector also went from 14% of the total incidents in the first quarter to only 10% of the incidents in the second quarter. The number of incidents for other industries included education (14%), government (13%), retail (12%), financial (10%), technology (9%), and all others (19%).

BREACH LEVEL INDEX

SECOND QUARTER RECAP 2014

WHAT IS THE BREACH LEVEL INDEX?

Not all breaches are created equal. Breaches are no longer a binary proposition where an organization either has or hasn't been breached. Instead they are wildly variable—having varying degrees of fallout—from breaches compromising entire global networks of highly sensitive data to others having little to no impact whatsoever.

The Breach Level Index not only tracks publicly disclosed breaches, but also allows organizations to do their own risk assessment based on a few simple inputs that will calculate their risk score, overall breach severity level, and summarize actions IT can take to reduce the risk score.

CALCULATING YOUR RISK ASSESSMENT SCORE

The Risk Assessment Calculator is a simple way to provide your inputs into the Breach Level Index in order to calculate your own risk score—indicating breach severity.
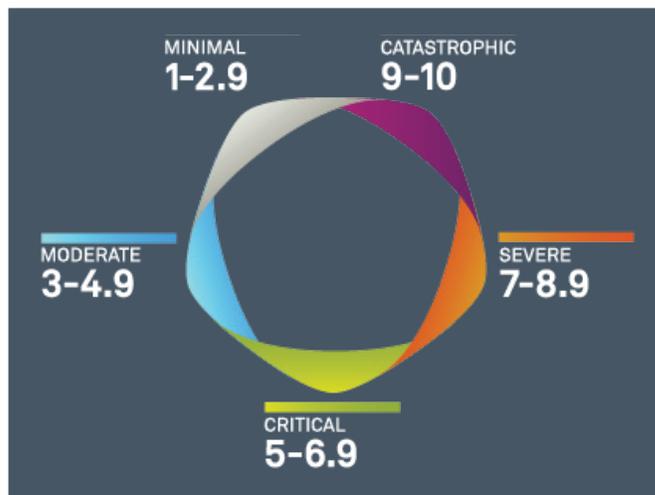
The very foundation of data security is evolving. It's no longer about "keeping the bad guys out and letting the good guys in" through breach prevention. More and more organizations are accepting the fact that despite their best efforts security breaches are unavoidable.

What's Your Score? Find Out At

BREACHLEVELINDEX.COM

RISK ASSESSMENT CATEGORIES

The first step in addressing the reality of a breach is focusing on the data itself. Since not all data is created equal, this means identifying, encrypting and controlling your most sensitive and high-value data assets.

Identify these categories for your organization:

- Total number of records breachable
- Type of data in the records
- Source of the breach
- How it can be exploited

SECURE THE BREACH

It's not a question if your network will be breached, the only question is when. With the velocity of business increasing, new technologies constantly being deployed and new and sophisticated attacks regularly being launched, is it not inevitable that it is only a matter of time before your business is hacked. - Learn more at: www.securethebreach.com

POWERED BY **SafeNet**