# BREACH LEVEL INDEX

## THIRD QUARTER RECAP
## 2014 (July - September)

## RECORDS BREACHED JULY - SEPTEMBER

# 183,375,285

## TOP SCORING BREACHES THIS QUARTER

| ORGANIZATION | RECORDS | TYPE | INDUSTRY | SCORE |
|---|---|---|---|---|
| *JP Morgan Chase* *(United States)* | 76,000,000 | Identity Theft | Financial | **10.0** |
| *Home Depot* *(United States)* | 56,000,000 | Financial Access | Retail | **9.8** |
| Online games, movie ticketing and ring tone website *(South Korea)* | 27,000,000 | Identity Theft | Technology | **9.6** |
| Community Health Systems, Inc. *(United States)* | 4,500,000 | Identity Theft | Healthcare | **8.9** |
| *Gmail* *(Global)* | 5,000,000 | Account Access | Technology | **8.6** |
| Affin Bank Berhad and Affin Islamic Bank Berhad *(United Kingdom)* | 1,271,000 | Financial Access | Other | **8.2** |
| *Salesforce* *(United States)* | 2,000,000 | Account Access | Technology | **8.2** |
| Japan Airlines *(Japan)* | 750,000 | Identity Theft | Government | **8.1** |

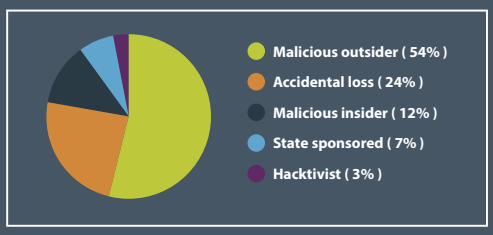
## WHAT THE PAST QUARTER REVEALED

According to publicly available information collected in the Breach Level Index, there were 320 data breaches and more than 183 million data records lost or stolen between July and September of 2014. Encryption was used in only 10 of the 320 reported data breaches, or less than 1%, where "secure breaches" with strong encryption, key management or authentication solutions rendered the data useless.

On average in Q3 2014, data records were lost or stolen with the following frequency:

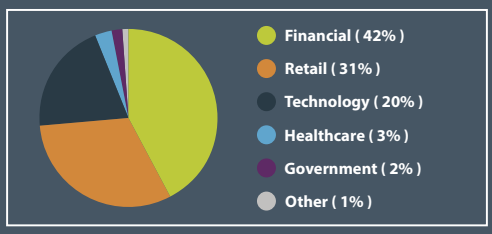
| Every DAY | Every HOUR | Every MINUTE | Every SECOND |
|---|---|---|---|
| 1,993,210 | 83,050 | 1,384 | 23 |

## TOP BREACH RECORDS BY SOURCE




MALICIOUS OUTSIDERS once again claimed the top spot for data breaches in the third quarter of 2014, accounting for 54% of all data breaches, and 95% of all the records accessed. This was followed by accidental loss (24%), malicious insiders (12%), state-sponsored (7%) and hacktivists (3%). IDENTITY THEFT was the leading type of data breach representing 45% of all incidents and 61% of records stolen.

## TOP DATA BREACHES BY INDUSTRY




Individuals also felt the data privacy pinch with breaches occurring across three major consumer activities: their banking, shopping, and online identities. The FINANCIAL sector led all industries in terms of records stolen with more than 77 million, accounting for 42%. Retail was close behind with more than 57 million (31%) in terms of the number of compromised customer accounts and data records. The retail industry had slightly less data records compromised than during their second quarter of 145 million records stolen or lost, or 83% of all data records breached, down to 57 million records or 56% of total records compromised. These were followed by breaches involving Technology and Personal Online Accounts (20%) such as email, gaming and other cloud-based services.

# BREACH LEVEL INDEX

## "MOVE FROM BREACH PREVENTION TO BREACH ACCEPTANCE"

Focus on the data itself.

## THIRD QUARTER RECAP 2014

## COUNTRY & REGIONAL PERSPECTIVES

North America had the most reported hacks - 211 incidents or 66%. Latin America reported the least with only 2 in Brazil and less than 1%. The United States had the most of any other country with 197 incidents or 62%, followed by the United Kingdom at 33 incidents or 10%, Canada 14 incidents 4%, Australia 11 incidents 3%, and Israel 10 incidents 3%. The U.S. lost almost 144 million records across a range of industries, representing 78% of all records lost. Other countries are catching up in reporting but are not as accurate. Possibly due to strict breach reporting laws in the U.S. compared to other countries.

## TOP ORGANIZATION BREACHES

**JPMorgan Chase.** Over the summer, hackers successfully got access to 76 million customer accounts, the equivalent of two-thirds of all American households. The breach exposed customer names, email addresses, phone numbers and addresses but did not include financial information.

10.0 Risk Score

**Home Depot.** Much in same fashion as previous retail data breaches, hackers likely compromised a third-party vendor to break into the retailer's in-store payments systems. More than 56 million credit card numbers were stolen at Home Depot, in what is the largest known breach of a retail company's computer network.

9.8 Risk Score

**South Korean "Extractor" Hack.** A group of hackers stole information affecting 27 million South Koreans through targeted attacks on registration pages for online gaming, movie ticketing and ring tone download websites. The data included the names, resident registration numbers, account usernames and passwords.

9.6 Risk Score

**Community Health Systems.** Hackers potentially associated with the Chinese Army used an Advanced Persistent Threat to get access into the healthcare provider's network and steal non-medical records of 4.5 million patients.

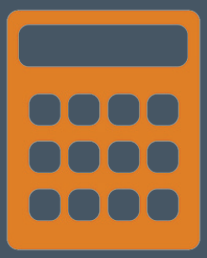
8.9 Risk Score

**Gmail Account Logins Posting.** The log-in credentials for 5 million Gmail accounts were posted online on a Russian web site. The credentials were likely stolen by phishing campaigns and unauthorized access to user accounts.

8.6 Risk Score

**Apple iCloud.** Celebrity accounts were compromised by what was very likely a brute force attack on user names, passwords and security questions, a practice that has become all too common on the Internet and has been successful because consumers or providers do not enable multi-factor authentication.

## 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.

Healthcare had 52 incidents or 16%, and less than 5 million records breached, less than 3%, meaning that the breaches that do occur in the Healthcare industry are "secure" or are keeping attackers from accessing information. Showing that they are an industry that takes breaches seriously and tries to protect them the most.

The financial services industry was hit hard due to the JPMorgan Chase breach. More than 77 million data records or 42% of all data records stolen, while only accounting for 11% of all data breach incidents with 33.

The government sector had the most amount of incidents at 72, or 23% of all incidents. Although it was pretty close across all sectors ranging from 10-23%. The number of incidents for other industries included education (11%), retail (14%), financial (10%), technology (12%), and all others (13%).

# BREACH LEVEL INDEX

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

## QUARTERLY RECAP 2014

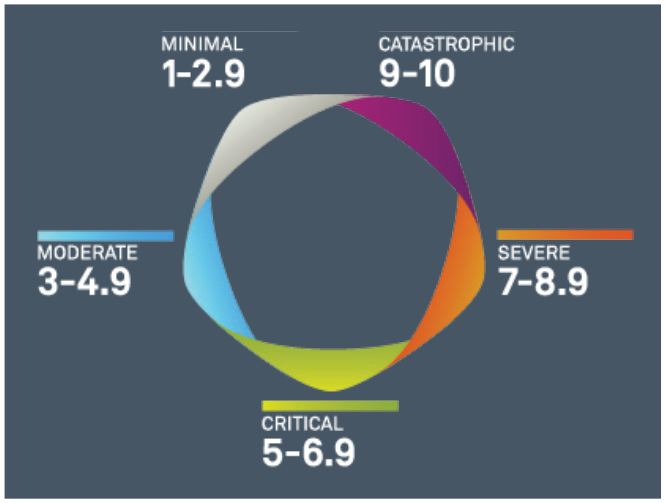
## WHAT IS THE BREACH LEVEL INDEX?

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

Information collected from public sources. SafeNet 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.safenet-inc.com**
**Follow Us:** www.safenet-inc.com/connected