ANNUAL RECAP
2013

BREACH LEVEL INDEX

RECORDS BREACHED

575,486,661

TOP SCORING BREACHES OVER THE PAST YEAR

Organization	Records	Type	Score
Adobe Systems, Inc. (U.S.)	152,000,000	Financial Access	10.0
Target (U.S.)	110,000,000	Financial Access	10.0
Country's Supreme Election Committee (Turkey)	54,000,000	Identity Theft	9.9
Cupid Media (Australia)	42,000,000	Identity Theft	9.8
Living Social (U.S.)	50,000,000	Account Access	9.3

WHAT THE PAST YEAR REVEALED

According to publicly available information collected in the Breach Level Index there were 1,056 data breaches and more than 575 million data records lost or stolen in 2013. This made 2013 a banner year with some of the largest data breaches ever, including Adobe (152 million), Target (110 million), Evernote (50 million) and Living Social (50 million).

On average in 2013, data records were lost or stolen with the following frequency: 47.9 million every month, 1.6 million every day, and almost 66,000 every hour.

The total number of 575 million data records lost or stolen actually underestimates the true scale of the problem of data security. That is because 44% of data breach incidents disclosed in 2013 did not indicate the number of data records exposed. In addition, many data breaches are never reported because they may be unknown to affected companies or organizations or contain records that are not sensitive enough to require notification to affected customers or users.
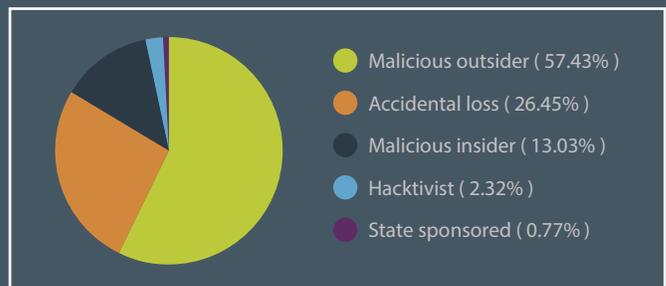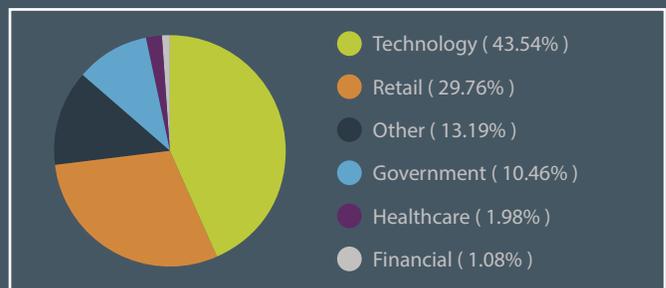
TOP BREACHES BY TYPE

In terms of the total number of data records lost or stolen, access to financial information claimed the top spot in 2013, accounting for 50% of all data records exposed. Financial information accessed included credit card, account or other financial information with potentially any of the following: name, mailing address, phone number, or email address. This was followed by account access (28%), identity theft (20%), existential data (1%), and nuisance (<1%). Looking at it in terms of the number of data breaches, identity theft led all others with 60%, followed by financial access (16%), account access (12%), nuisance (8%), and existential data (4%).

TOP BREACH INCIDENTS BY SOURCE

Malicious outsiders claimed the top spot for data breaches in 2013, accounting for 57% of all data breaches. This was followed by accidental loss of data (26%), malicious insider (13%), hacktivist (2%), and state sponsored (1%).

- Malicious outsider (57.43%)
- Accidental loss (26.45%)
- Malicious insider (13.03%)
- Hacktivist (2.32%)
- State sponsored (0.77%)

TOP BREACH RECORDS BY INDUSTRY

- Technology (43.54%)
- Retail (29.76%)
- Other (13.19%)
- Government (10.46%)
- Healthcare (1.98%)
- Financial (1.08%)

The healthcare sector led all industries in terms of the number of data breach incidents with 31%. This was followed by government (17%), technology (10%), financial services (10%), and retail (8%).

BREACH LEVEL INDEX

POWERED BY **SafeNet**

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

ANNUAL RECAP 2013

NOT ALL BREACHES ARE CREATED EQUAL

2013 demonstrated the fact that not all breaches are created equal. While healthcare (31%) and government (17%) were the top two industry sectors in terms of the number of data breaches, technology and retail were the top two sectors in terms of data records lost or stolen with 44% and 30%, respectively. The technology sector had more than 249 million records lost or stolen and the retail sector had more than 170 million records lost or stolen. In addition, technology and retail also lead all other industries in terms of data records lost per breach averaging 2.4 million and 2.1 million records lost per breach, respectively.

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.

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

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.

MINIMAL 1-2.9

CATASTROPHIC 9-10

MODERATE 3-4.9

SEVERE 7-8.9

CRITICAL 5-6.9
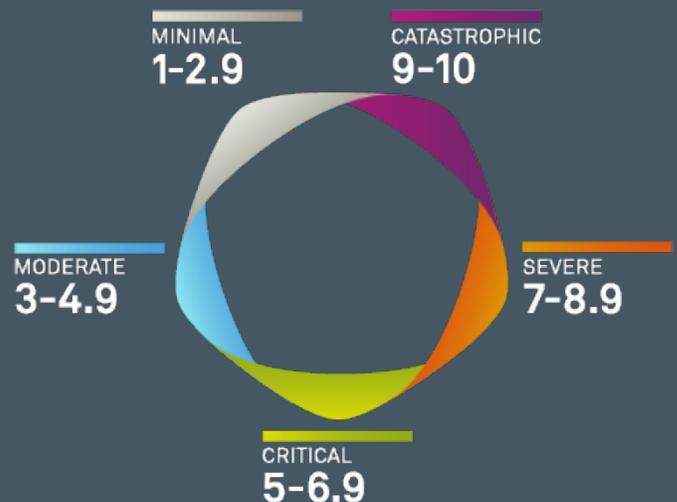
The very foundation of data security is evolving. It's no longer about "keeping the bad guys out and letting the good guys in" through breach prevention. More and more organizations are accepting the fact that despite their best efforts security breaches are unavoidable.