

Categorizing Data Breach Severity with a Breach Level Index

Richard Stiennon
Founder, IT-Harvest

Abstract

Data breaches have become a common occurrence, and the reality of the problem is much worse than current perceptions, because the general population is only aware of publicly disclosed breaches. It is not aware of the multitudes of breaches that either are not under any disclosure mandate, or breaches that have not yet been detected. The latter category is a very large number, since most research shows that it can take months or even years before an organization detects a breach.

As regulations and security infrastructure have evolved to face this problem, so too has the nature of breaches. Breaches are no longer a binary proposition where an organization either has or hasn't been breached. Instead they are wildly variable in their severity and ramifications both to the breached organizations and their core constituencies and partners. This environment demands some sort of tool that can indicate breach severity – because we are in an era where fool-proof breach prevention is simply not a realistic expectation. Instead, we need to examine breaches on a case-by-case basis to fully understand their severity.

To accomplish this goal, IT-Harvest and SafeNet undertook a joint project to develop the Breach Level Index (BLI). The Breach Level Index is designed to provide a simple way to input publicly disclosed information on data breaches and calculate a score indicating breach severity. The methodology behind the Breach Level Index is defined in this document, and we welcome security professionals to test the formula and contribute their thoughts to its evolution.

The Need for the BLI

Breach reporting is mandated in 46 states in the United States and legislation is pending or being enacted in several countries around the world (i.e., Netherlands, Australia, UK, EU). These requirements have led to more transparency and what seems like a constant stream of breaches in the news. While the severity of a breach depends on many factors – including the type of information involved, the threat actors, and whether or not the lost or stolen data is actually used to cause harm – the media tends

to focus on total number of people impacted. This is certainly a legitimate factor, but the other factors also need to be taken into account to move beyond the “one size fits all” perception of breaches and into a more productive discussion.

With that in mind, IT-Harvest, with the support of SafeNet, has endeavored to create a Breach Level Index that can help to put different breaches in perspective.

Background: Other Scales Provide a Framework

There is plenty of precedent for creating scales to help identify the severity of damaging events, ranging from burn degrees in medicine to natural disasters in meteorology. For example, wind severity is classified by the Beaufort Scale, volcanic eruptions by the Volcano Explosivity Index, earthquakes by the Richter Scale and, probably the best known, the hurricane Saffir-Simpson scale.

The Beaufort Scale is the oldest such scale, created in 1805 by Francis Beaufort, an Irish Royal Navy officer. When Beaufort became a top administrator in the Royal Navy in the 1830s it was officially adopted and first used during the voyage of HMS Beagle under Captain Robert Fitzroy. The Beaufort Scale was used in reporting wind conditions and ranges from Force 0 (calm) to Force 12 (hurricane).

Developed in 1935 by Charles Richter in partnership with Beno Gutenberg, both from CalTech, the Richter scale is based on the logarithm of the amplitude of an earthquake measured on a seismograph. Barely perceptible earthquakes fall in the 2-3 range, while anything above 7 can be extremely destructive.

The Saffir-Simpson scale for the well known hurricane categories was created in 1969 by Herbert Saffir, a consulting engineer, and Dr. Bob Simpson, director of the National Hurricane Center. It is a simple delineation of hurricane severity based on potential damage to buildings and storm surge, with a Category 1 being the least severe and a Category 5 the most.

Volcanic eruptions are measured in severity by the amount of material ejected during the eruptions. The Volcanic Explosivity Index (VEI) was created in 1982 by Chris Newhall of the U.S. Geological Survey and Stephen Self at the University of Hawaii. The lowest VEI (0) indicates less than 10,000 cubic meters of material. The current eruptions in Hawaii meet this measure. Mount St. Helens ranked a 5 with more than a cubic kilometer of ejecta, and Krakatoa a 6, almost 10 times greater.

Log10 (N x t x s x A)
Where:
N= the total number of records breached, or, in the case of intellectual property loss the equivalent dollar loss.
t= the type of data in the records <i>values</i> <ol style="list-style-type: none"> 1 Nuisance (email addresses, affiliation, etc.) 2 Account access (username/passwords to social media, websites, etc.) 3 Financial access (bank account credentials, credit card data) 4 Identity theft (information that can be used to masquerade as someone) 5 Existential data (information of national security value or threatens business survival)
s= source of the breach <i>values</i> <ol style="list-style-type: none"> 1 Lost device such as a laptop, DVD, or USB thumb drive 2 Stolen device 3 Malicious insider 4 Malicious outsider 5 State espionage
Action= whether or not the stolen data has been used to cause harm be it identity theft, credit application, or bank account withdrawals <i>values</i> <ol style="list-style-type: none"> 1 No action 5 Publication of embarrassing or harmful information (Wikileaks, hacker logs, etc.) 10 Use of financial identity to obtain funds or apply for loans

Breach Level Index Methodology

The Breach Level Index has to be inclusive of minor loss of data all the way up to the largest reported breaches, such as that of the 150 million records stolen from the Shanghai Roadway Marketing Service reported in March 2012.

The Breach Level Index must fit the information readily available for each breach and it must be easy to understand and calculate. It should include weighted values for number of records, type of data, source of the breach and whether or not the data has been used for nefarious purposes.

The Breach Level Index is open ended in that there is no upper limit, although to date the largest breach scores just under a 10. The Index is logarithmic (base 10) so just as in the scales for volcanoes and earthquakes, a score of 7, for instance, is 100 times more severe than a score of 5. To see how it plays out, here is a table showing the scores of several historical breaches:

Organization	Number of Records Breached (N)	Type of Data (t)	Breach Source (s)	Action (A)	Breach Level Index Score
Zappos	24,000,000	3 - Credit Card or Debit Card Information, Login Information, Email, Addresses, Phone Numbers, Other Personal Information	4 - Outsider – Malicious	1	8.5
Global Payments	1,500,000	3 - Credit Card or Debit Card Information	4 - Outsider – Malicious	10	8.3
State of South Carolina	5,800,000	4 - Social Security Numbers, Account Information, Credit Card or Debit Card Information	3 - Insider – Malicious	1	7.8
FBI	12,000,000	1 - Names, Phone Numbers, Addresses	4 - Hacktivist	1	7.7
New York State Electric and Gas	1,800,000	4 - Social Security Numbers, Account Information, Dates of Birth	4 - Outsider – Malicious	1	7.5
Nationwide Insurance, Allied Insurance	1,100,000	4 - Social Security Numbers, Names, Dates of Birth, Other Personal Information	4 - Hacktivist	1	7.2
Yahoo	400,000	2 - Login Information	4 - Hacktivist	5	7.2
LinkedIn	1,500,000	2 - Login Information	4 - Hacktivist	1	7.1
U.S. Federal Government	1,600,000	2 - Account Information, Names, Login Information, Email, Phone Numbers	4 - Hacktivist	1	7.1
CA Dept. of Children Support Services	800,000	4 - Social Security Numbers, Medical Records, Names, Addresses, Other Personal Information	1 - Insider – Non-Malicious	1	6.5

Taking a Final Step

To make the Breach Level Index easily understandable to a broad swath of society, we think it makes sense to map the Index scores to a simple five-step scale, similar to the Saffir-Simpson scale. The following table shows how Index scores map to this scale. To put it into context, the California Department of Support Services breach would be a Category 3 data breach, while the LinkedIn breach would be Category 4.

Category	Breach Level Index Score	Characterization
5	9-10	Breach with immense long term impact on breached organization, customers and/or partners. Very large amount of highly sensitive information lost (usually 10-100+ million records). Massive notification process. Potentially existential financial loss for breached organization in remediation and related costs. Use of lost sensitive information seen.
4	7-8.9	A breach with significant exposure to business, Legal and/or regulatory impact. Large amount of sensitive information lost (usually hundreds of thousands to millions of records). Significant notification process costs involved and public image impact.
3	5-6.9	A breach with likely short to midterm exposure to business. Legal and/or regulatory impact. Usually tens of thousands of records of moderate sensitive information involved. Some breach notification and financial loss.
2	3-4.9	A breach with low long-term business impact. Usually involves the loss several thousands of records of semi sensitive information. Limited breach notification and financial exposure.
1	1-2.9	A breach with no material effect. Less than one thousand records. breach notification required, but little damage done.