Overview: As data breaches continue to threaten the safety of information and corporate infrastructure, risk assessment for data is no longer a nice-to-have—it is a must have. Data mapping, the process of electronically identifying and organizing data, can minimize the impact of a data breach by allowing organizations a clear understanding of the location, format and security level of their important data.

In early July of 2015, the U.S. Office of Personnel Management (OPM) was faced with a catastrophic data breach. The OPM reported that files of more than four million former and current federal employees had been hacked. According to the formal report, this meant that, “information such as full name, birth date, home address, and Social Security numbers” were out on the open market.

During the scramble to mitigate the damage of this breach, the OPM launched a full investigation into the security of the department’s data. They found an additional cache of data that had been hacked in a repository not previously considered in the OPM’s initial impact assessment. This new repository contained a huge amount of Social Security Numbers (SSNs), spouse names, and even fingerprint records—bringing the number of affected individuals to more than 21.5 million in a matter of hours.[2]

This revelation added fuel to the media debacle because the OPM had seemed to initially “understate” the breach impact. This was not a piece of valuable information that the OPM simply chose to ignore, they simply didn’t know at the time. The OPM’s breach event supports the Inspector General’s warning in
2014: put a simple security measure in place—a data map. Without an inventory of OPM’s servers, databases, and hardware, the OPM had no accounting for the thousands of pieces of information being exchanged and infiltrated every day. A data map could have saved them millions of dollars in data investigation and remunerative fees, notwithstanding the security “black eye” which they could have lessened or avoided altogether.

Unfortunately, too many of these breaches have shown how little even very large-scale organizations seem to know about their data. Without a clear understanding of the total data picture, any organization is more vulnerable to unsuspected and devastating attacks that can affect its reputation and financial stability.

**Sophisticated Threats and Unsophisticated Data Management**

As much as some information specialists would like to prove that cybersecurity has kept pace with the activities of data threats, history has proved otherwise and organizations of all sizes are at risk. The recent breach of 80 million healthcare records held by Anthem Blue Cross exposed the company’s entire database to malicious activity, making SSNs, addresses, and income data available to the highest black-market bidder. Today, selling identities is more lucrative than selling drugs, causing a dramatic influx of criminals seeking to steal data.

But, increased identity theft is just one of the costs of data mismanagement. In the 2015 survey from the Ponemon Institute, the average notification cost of one “run-of-the-mill” record in a data breach is $145–$155, up 6% from 2014. The cost increases dramatically if records are compromised by malicious activity, such as identity theft or credit fraud, to an average cost greater than $300 per record. In addition, the information stolen in these kinds of attacks can have long-lasting negative effects on client–customer relationships, leading to decreased business volume and customer confidence.