FIVE BIG DATA SECURITY CONSIDERATIONS

NO ONE DOUBTS THE POTENTIAL BUSINESS VALUE OF BIG DATA ANALYTICS, A MULTI-BILLION-DOLLAR OPPORTUNITY, IN THE ENTERPRISE, BUT WITH GREAT POTENTIAL COMES GREAT SECURITY RISK. READ ON TO LEARN MORE ABOUT THE TOP FIVE BIG DATA SECURITY CONSIDERATIONS TODAY.

The security concerns surrounding Big Data in highly regulated industries are numerous, to say the least. At times, more questions than answers seem to abound, so where should enterprises start to glean actionable intelligence from Big Data analytics while keeping a firm hold on information security? This article highlights five key Big Data security considerations and where enterprises can find an expert partner to navigate the ever-evolving threat landscape.

BIG DATA ANALYTICS IS A MULTI-BILLION-DOLLAR OPPORTUNITY AND KEEPING A FIRM HOLD ON INFORMATION SECURITY IS KEY

IIS TECHNOLOGY
MISSION POSSIBLE

NAVIGATING THE REGULATORY LANDSCAPE WILL REQUIRE FLEXIBLE, AGILE SOLUTIONS

Highly regulated industries, such as finance and health care, have

ıavigate a constantly shifting regulatory environment, particularly when it comes to information security and privacy protections. The Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPPA) are only two of the biggest challenges enterprises face, and with respect › Big Data and advanced analytics, these challenges are only becoming more complex (or confusing) with each updated, new or outdated regulation.

The proliferation of data lakes (i.e., large, specialized Big Data repositories for "dumping" data to be used for analytics at a later date) is becoming more common as enterprises continue to find substantial value in Big Data analytics. Some of the primary security concerns revolve around how enterprises should store these data in the first place while managing who can access these data and at what time and for how long.

The solutions to these seemingly rudimentary considerations are easier said than done given the fact that no one knows what the regulatory landscape will look like a decade from now. As such, enterprises will need to consider flexible, adaptable and agile open-source solutions to the governance, regulation and compliance conundrum to keep pace with regulations in the future.

1

NAVIGATING THE REGULATORY LANDSCAPE WILL REQUIRE FLEXIBLE, AGILE SOLUTIONS

2

BALANCING ANALYSTS' REQUIREMENTS WITH SECURITY CONCERNS

3

IT IS GARBAGE IN, GARBAGE OUT ONCE AGAIN?

BALANCING ANALYSTS' REQUIREMENTS WITH SECURITY CONCERNS

Often, this aspect of Big Data revolves around who owns and is responsible for which data and who should have access to data housed elsewhere in the enterprise. More often than not, this reality creates friction between analysts and data scientists, who need unfettered access to complete data sets to perform predictive analytics, and those responsible for data security within a particular line of business. From a high-level point of view, restricting access to certain data repositories defeats the entire purpose of Big Data analytics.

If enterprises apply encryption to all data, both classified and non-classified, what is the best way to ratchet encryption up or down? Regulations, such as HIPPA, overtly require data encryption regardless of an enterprise's choice to encrypt data or not. The risk of restricting access to certain data is that analysts may not be working with all the data necessary to glean the most value from Big Data insights. In a worst-case scenario, this shortcoming can lead to a multi-million-dollar mistake.

IT IS GARBAGE IN, GARBAGE OUT ONCE AGAIN? THINK TWICE...

In the IT world, "garbage in, garbage out" has become a mantra, and with respect to Big Data security, this time-tested wisdom still applies. The question remains: Who will determine which data are negligible and which data should be kept by enterprises? Big Data analytics require veracity over the long term, so when analyzing a broad and deep data set, who can say which data will not be important in the future? The answer is all data have value.

> **"ALL DATA HAVE VALUE."**

Today, there is no such thing as garbage or junk when it comes to Big Data. Data that appear marginal today may have substantial business value in the future. The capabilities of Hadoop, among other software development platforms, step forward as one solution to simply managing and preparing data for analysis over the long term. The risk is that without an agile tool, enterprises may once again be missing out on a critical opportunity to monetize Big Data insights. Enterprises can and should be keeping all data.

THE KEY ROLE OF OPEN SOURCE

Along the lines of Hadoop, among other platforms, open source and Big Data go hand in hand. In one manner of speaking, Big Data cannot be successfully analyzed without open-source solutions. Cloud has benefited greatly from the open-source movement, a benefit that will only trickle down to Big Data analytics in the cloud.

Security at the application level must become central to any Big Data initiative. Depending on a company's particular industry, this consideration may be critical or less important. For instance, identity management remains a huge concern in a financial application. On the contrary, identity management may not be as critical in a Big Data-driven marketing application. Big Data does not excuse enterprises from these long-standing security concerns. Open source can enable a more efficient way to balance security and identity management, particularly when leveraging the cloud.

4

THE KEY ROLE OF OPEN SOURCE

THE QUESTION OF TALENT

THE QUESTION OF TALENT

Often, Big Data security requires real-time solutions with respect to highly regulated industries. The anticipated shortage of Big Data talent will only trickle down to security concerns. In short, enterprises will not be able to find talented "off the shelf" programmers and analysts. The skill set required, such as programming expertise and business acumen, is simply difficult to find in any one individual. The key issue with Big Data security will be how enterprises can develop and build teams in-house to tackle the security conundrum.

> ***"THE KEY ISSUE WITH BIG DATA SECURITY WILL BE HOW ENTERPRISES CAN DEVELOP AND BUILD TEAMS IN-HOUSE TO TACKLE THE SECURITY CONUNDRUM."***

IIS's proactive consulting services can provide precisely this capability. Reactive management of security issues will lead only to inefficiencies and missed opportunities. With IIS, enterprises can receive the consultation needed to build Big Data security teams, enabling success for years to come.

Visit www.iisl.com for more information on how IIS's expertise stands apart from the rest.

IIS TECHNOLOGY
MISSION POSSIBLE