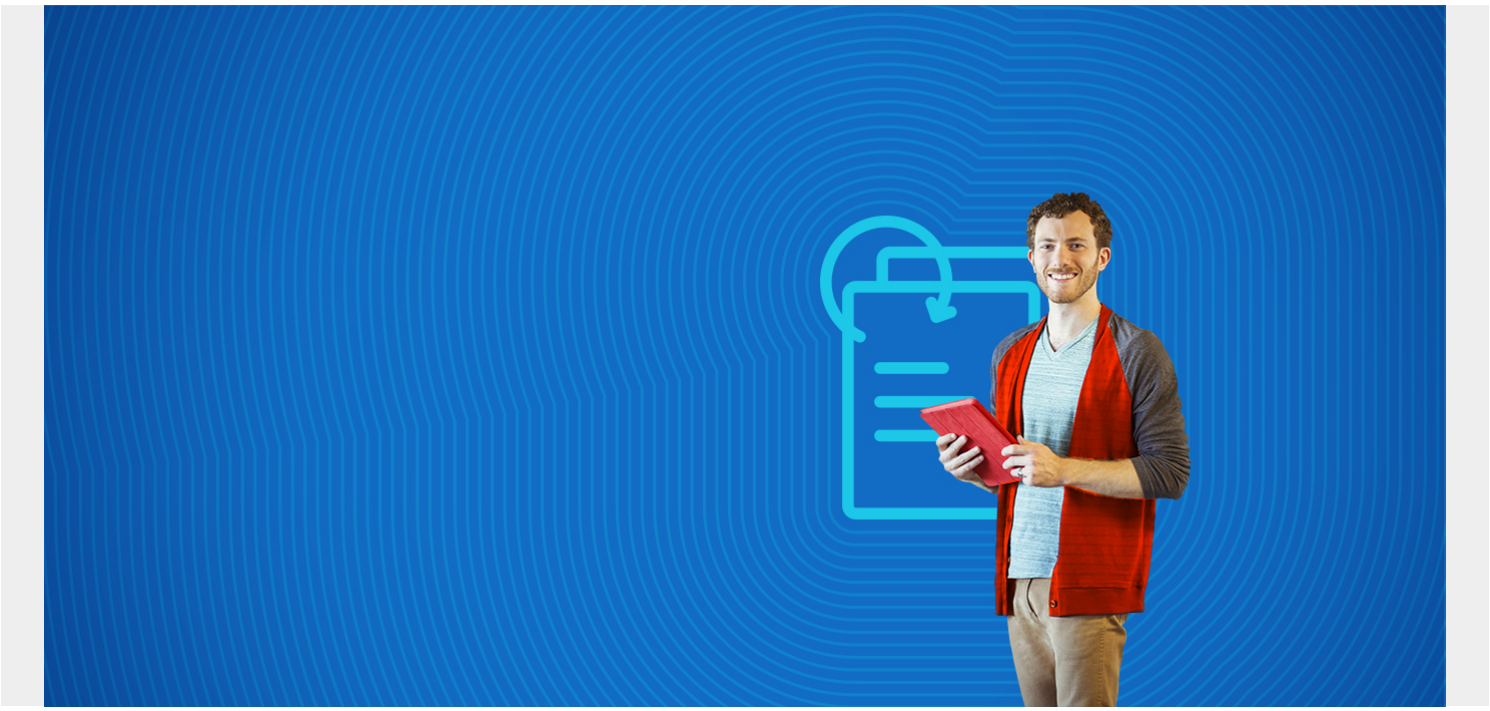
BIG DATA SECURITY ISSUES IN THE ENTERPRISE



Big Data promises vast improvements to business operations and lets organizations deliver tailored services for every customer. The exploding volume of information generated via social media and connected sensors contain patterns of hidden insights that can be transformed into tangible business benefits. This transformation requires added efforts associated with data collection, processing, analysis, storage and security. The advantages of Big Data also come with pressing implications that organizations must consider maximizing the value potential of their Big Data initiatives. Also, sophisticated cybersecurity threats and stringent privacy regulations further necessitate organizations to walk the extra mile in securing their Big Data systems and environment. These security challenges and issues can fall in the following key areas:

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

1. Securing the Environment

Big Data is distributed by nature. The vast volumes of data generated at virtually limitless sources make Big Data geographically distributed. The data is often collected and stored at locations closer to the source of generation for reasons associated with latency, processing and analysis delays, and data transmission limitations, among others. Operating on-premise servers in a geographically distributed environment may require additional security measures due to more moving pieces, dynamically distributed workloads, traffic fluctuations and configuration updates. For customers of cloud based services, organizations may have limited visibility and control into the security initiatives necessary to protect data across borders. Integration of complex distributed IT infrastructure resources make security measures an additional challenge. Businesses investing in Big Data projects must therefore evaluate the challenges associated with security and infrastructure complexity of a

distributed IT environment, which may be critical for the success of any Big Data initiative.

2. Security Loopholes in the Log Metrics Big Data Cosmos

The accuracy and integrity of the Big Data has an immediate impact on the business decisions, forcing organizations into taking actions that may undermine the business performance or IT security. Consider the case of complex IT infrastructure that generates a deluge of log data. This data contains valuable information regarding traffic flows across the network and details regarding apps, services and users accessing the infrastructure resources. When organizations develop Big Data projects without placing adequate security measures, loopholes within the network, access management or security policies allow cybercriminals to compromise the network or data. For instance, without adequate log analytics and incident management capabilities, organizations may not be able to identify the red flags identifying anomalous traffic activities.

3. Data Security in Real-Time

The Big Data generated or collected may present immense value to organizations even before it's processed and analyzed. Since the data is not always generated within secure networks and the data at transit must be protected from threats in real-time. For instance, a sensor network taking critical measurements beyond the organizational network may be compromised to leak data or yield false data streams. The data may be processed as it is received and the technical or business decisions are made according to the resulting insights based on false or compromised data. Without a data integrity system in place, relying on false data to perform critical decisions on business operations can have severe implications not only to the organization but also for its customers and end-users. Additionally, many cyber-attacks exploit data while it's in transit within weak public networks. For business organizations and relevant stakeholders, securing the Big Data supply chain end-to-end may not always be a financially viable solution and therefore leave doors open for cyber-attacks.

4. Exercising Due Diligence

Big Data initiatives require organizations to invest in a range of enterprise IT technologies, including cloud infrastructure and SaaS offerings. These services are used to store and process sensitive data and should therefore maintain the necessary security measures. Adequate due diligence is required to ensure that these vendors fulfil the criteria, but for small and midsize firms lacking the necessary resources, finding the right vendor capable of maintaining data security may be difficult. Additionally, organizations running fast growing Big Data projects may run into challenges associated with vendor lock-in and integration. Some vendors make it easier to enter the service but difficult to integrate it with their competitors or expensive to move out of the service. And when these vendors fail to promise adequate security defense capabilities growing threats, organizations may risk data exposure in attempts to drive down the technology cost.

5. Backups and Business Continuity

In order to ensure business continuity, organizations invest in backup, disaster recovery and redundancy systems to ensure that the necessary data is always available during and after disaster situations. For Big Data projects, the cost of these necessary security capabilities grows

exponentially with the rapid and exponential growth of useful data. And even when organizations are committed to invest in these capabilities, the data backup and restoration process becomes time consuming and complicated for large volumes of data. In event of disaster, the services dependent upon Big Data may remain unavailable until the large volumes of information is fully recovered from backup sites.

Maintaining security of Big Data projects operating within distributed computing frameworks face the added challenge for business continuity. With more points of failure present across geographic boundaries, organizations must ensure reliability of systems facing different levels of business continuity challenges. For instance, each geographic zone may require its own set of Recovery Point/Time Objectives based on risk of power outages, natural disasters and cyber-attacks.

6. Preserving End-User Privacy

While Big Data associated with every customer allows organizations to deliver better services and improved end-user experience, customers may not always allow the collection and use of their private information for business purposes. Stringent regulations such as the GDPR have imposed strict limitations in the way business organizations can collect, process and share customer data. In event of a security breach, organizations now face strict legal action and heavy fines that could potentially fail a business altogether. The challenge for business organizations therefore is to take extra measures in securing privacy-sensitive Big Data and ensure that data collection and use is in line with the regulatory compliance requirements.

An effective Big Data strategy should therefore establish an optimal tradeoff between data security, resource investments and business performance. Technical capabilities such as real-time security monitoring, granular audits and access controls, and other proactive measures for business continuity and risk management will be critical to the success of Big Data initiatives.