Cyber Security and Data Governance Best Practices for Today's Data Environment

A network of hurdles dominates the current data environment. Rapid data growth makes data difficult to manage. Meanwhile, cyber-attacks grow increasingly sophisticated and frequent, while remote work and cloud migration complicate the security landscape. Now, more than ever, cyber security and data governance best practices play a critical role.

In 2020, the world generated approximately 2.5 quintillion (that's 2.5 billion billion) bytes of data. Data analytics hold a world of promise. However, the data comes so quickly and in such volume that organizations struggle to harness its value and keep it safe.

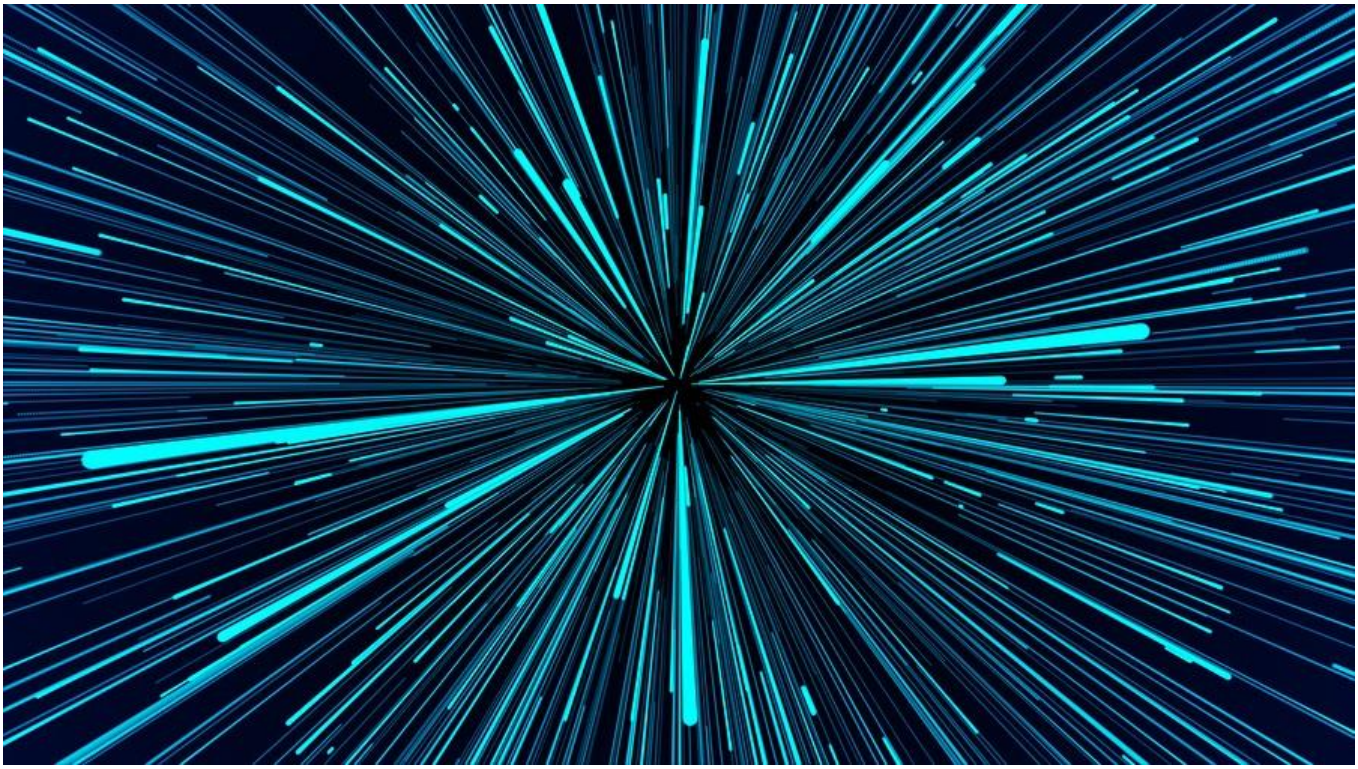
Data governance thus becomes a critical priority. Organizations must develop strong data governance programs, including robust cyber security, to turn data into a business asset rather than a costly liability. These best practices will help.

Understand Business Priorities and Risks

To ensure success, businesses should tailor security and governance strategies to match business goals and identified risks. With representatives of each major area of the company, begin by answering some key questions.

For instance, determine business priorities and problem areas from each department. That is, what goals can data help to solve, and what keeps the organization from gaining value from its data?

Additionally, discover the state of data security within the organization, identifying weaknesses. This will involve examining the company's incident response plan and security procedures, including backups and encryption. A comprehensive risk analysis will help at this stage. Also, determine where data lives, who has access to it and what regulations govern its use.



Automate Data Governance Tasks

To ensure quality data and improve compliance, organizations need to find and catalog data and track its movement over time. Those processes can prove prohibitively time consuming with huge amounts of data entering the system from a wide variety of sources. Automated tools that use AI and machine learning can save time and money and improve data quality.

For instance, machines can scan data for errors or omissions in a fraction of the time it would take data analysts to perform the same task. Additionally, automating data discovery and data lineage with a combination of metadata and AI increases data visibility and accuracy.

Take Responsibility for Ensuring Security in the Cloud

By some estimates, 92 percent of businesses use cloud services in some form. While cloud migration has empowered remote work and business agility, it presents security challenges. Many organizations do not realize that the default cloud security tools offered by cloud providers do not provide sufficient security.

Organizations also need to understand that they share responsibility for cloud security with their cloud providers. For instance, depending on the type of services provided, the organization may be responsible for ensuring full encryption and managing user access to data. Companies should work closely with cloud providers to ensure appropriate data protection strategies.

Protect Data by Carefully Managing Data Access

When determining access, protect critical data by restricting user access to just the data and systems needed to complete their jobs. Too often, users have far more access than necessary, and that creates significant risk. Applying role-based access and the principle of least privilege helps to minimize that risk and ensure regulatory compliance.

In conjunction with least privilege, implement zero trust policies, which require authentication of all users and devices, every time. When organizations store data both on premises and in multiple cloud environments, traditional network boundaries disappear. Zero trust uses technologies such as multi-factor authentication (MFA) to verify identity.

Build Communication into the Process

Successful security and data governance programs depend on people, from executive champions to end users. Start by involving C-level executives and key stakeholders from the very beginning. Ensure engagement by clearly communicating the business value of clean, organized, and secure data, as well as the risks of insufficient data security.

Commit to ongoing transparency, communicating governance strategies, as well as progress against data governance goals and security challenges. This involves users from the executive level down to the summer intern. Conduct regular employee education to ensure that they understand data policies and their roles in relation to data, including data security.

Make Security and Data Governance Best Practices an Ongoing Priority

Ultimately, data governance involves creating data value by ensuring that data is well-organized, high-quality, and secure from attack. Commit to the long haul by regularly assessing and revising data governance and security goals and programs.

The data governance and security experts at Messaging Architects can help. With proven tools and methods for data management, cyber security, and compliance monitoring, they have helped hundreds of organizations reduce risk and realize data value.