Link Data Governance and Cybersecurity to Protect Valuable Data Assets

In today's business environment, data ranks near the top of the list of most valuable assets. It drives development strategy, focuses marketing efforts, and even saves lives. Cyber criminals know well the value of data and its power to make or break an organization. Consequently, organizations must link data governance and cybersecurity to stay ahead of the game.

Data Governance and Cybersecurity Defined

Think of data governance and cybersecurity as overlapping circles. Though distinct concepts, they share common goals and depend on each other.

Data governance involves an organization knowing what data it owns, where that data lives and who owns and uses it. It also encompasses the processes of ensuring the integrity and availability of data, as well as its classification.

Cybersecurity, on the other hand, refers to protecting networks and data from unauthorized access and criminal use. It involves a combination of technology, people and processes working together to prevent and mitigate cyber-attacks.

Data governance and cybersecurity share a common goal of protecting valuable data assets, making quality data available to the right people at the right time. In an environment increasingly influenced by privacy regulations and big data, proper handling of data can have significant repercussions.

Cybersecurity Landscape Has Evolved

Not so very long ago, security experts spoke in terms of castle and moat security. Also known as perimeter security, this strategy involved using multiple defense layers to fortify the perimeter surrounding the data network. Firewalls, honeypots and other intrusion prevention devices guarded the various points of access into the system.

However, the cybersecurity environment has evolved substantially, rendering castle and moat security ineffective. Now security professionals must account for a variety of complicating factors, including:

- Data explosion – The amount of data generated daily has grown exponentially over the last decade, thanks in part to the IoT. By some estimates, data volumes will reach 175 zettabytes by 2025. Half of that data will live in the cloud.
- Data privacy – The introduction of GDPR in 2018 turbo charged the data privacy movement. Now, nearly every organization must address compliance with one or more privacy acts, from GDPR to HIPAA to CCPA, PCI DSS and more. Data privacy and cybersecurity have become closely intertwined.
- Remote Work – With a significant percentage of the workforce working remotely, organizations must balance productivity and data accessibility with security. Issues surrounding cloud storage and remote connections take center stage.
- Ransomware, phishing, and other threats – Cyber criminals continually up their game. Using much more sophisticated methods than before, they launch targeted attacks at an unprecedented rate. In fact, a recent FBI report indicates a 69.4 percent increase in suspected internet crime from 2019 to 2020.

Essential Role of Data Governance in Effective Cybersecurity

In this evolving data landscape, data governance plays a critical role in implementing security strategy. To protect sensitive data and comply with complex regulations, organizations must first know where the data resides and who controls it. Proper organization of data both reduces the risk of data breach and aids in forensics when security incidents do occur.

For instance, metadata tags can be used to flag sensitive data and initiate access controls and archiving. This helps to prevent unauthorized access. It also creates an audit trail and ensures compliance with data retention requirements.

Getting Started with Data Governance

Building data governance into the corporate culture takes time. Start by securing executive sponsorship, as effective data governance requires coordination among departments. Then begin with small projects, such as email.

The consultants at Messaging Architects can help you include data governance as an integral part of your overall cybersecurity strategy. A comprehensive audit will give you a map of the data landscape. Then ongoing data management and compliance monitoring will provide necessary visibility to reduce risk moving forward.

Contact Messaging Architects to begin implementing a robust data governance strategy that will drive cybersecurity and support business goals.