Examining the Data Trinity: Governance, Security and Privacy

A strong data governance foundation underpins data security and privacy

erwin®
the data governance company

Learn More at
erwin.com

Introduction

Data breaches continue to make headlines.

Without the appropriate data security protections and controls, organizations potentially will have to deal with the fallout of failing to protect the personal information of their customers. That's bad corporate citizenship not to mention terrible PR. Of course, media coverage of security cracks that lead to the cybertheft of corporate intellectual property is harder to find, since businesses tend to keep these incidents under wraps. But a hit like that can take a significant toll on a company's value.

Such incidents may be the result of not having a true data governance foundation that makes it possible to understand the context of data—what assets exist and where, the relationship between them and enterprise systems and processes, and how and by what authorized parties data is used. This knowledge is critical to keeping relevant data secure and private so companies are regarded as responsible data stewards by customers and remain in compliance with such regulations as Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

Creating policies for data handling and accountability and driving culture change so people understand how to properly work with data are two important components of a data governance initiative, as is the technology for proactively managing data assets. Without the ability to harvest metadata schemas and business terms; analyze data attributes and connections; impose structure on definitions; and view all data in one place according to each user's role within the enterprise, businesses will be hard pressed to stay in step with governance standards and best practices around security and privacy.

As a consequence, the private information held within organizations will continue to be at risk. Organizations suffering data breaches will be deprived of the benefits they had hoped to realize from the money spent on security technologies and the time invested in developing data privacy classifications. They also may face heavy fines and other financial consequences. For example, the U.S. Securities and Exchange Commission levied a $35 million fine on Altaba Inc.—the new name of Yahoo that hosts the business' assets that were not acquired by Verizon—for non-disclosure of the 2014 data breach to investors. Meanwhile, Verizon walked away with Yahoo's technology and web properties for $350 million less than the original purchase price.

Unfortunately, businesses don't have visibility across their full data landscapes—linkages, processes, people and so on—to propel more context-sensitive security architectures to fulfill expectations for user and corporate data security and privacy. They lack the ability to connect the dots across the data trinity—governance, security and privacy—and to act accordingly.

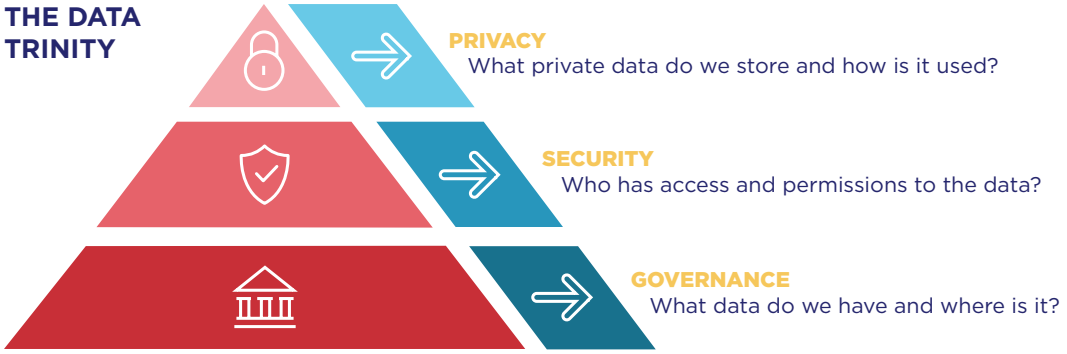
Governments Also Plagued by Data Breaches

Governments don't always practice smart data governance either. Some of the most egregious breaches have occurred both at the U.S. state and federal levels and are as follows:

- **U.S. Voter Database:** 191 million affected (December 2015)
- **National Archives and Records Administration (NARA):** 76 million affected (October 2009)
- **U.S. Department of Veteran Affairs:** 26.5 million affected (May 2006)
- **U.S. Office of Personnel Management (OPM):** 21.5 million affected (June 2015)
- **Virginia Department of Health Professions:** 8.3 million affected (May 2009)
- **Office of the Texas Attorney General:** 6.5 million affected (April 2012)
- **Georgia Secretary of State Office:** 6.2 million affected (November 2015)
- **Tricare:** 4.9 million affected (September 2011)
- **South Carolina Department of Revenue:** 3.6 million affected (October 2012)
- **State of Texas:** 3.5 million affected (April 2011)

Data Puzzles and Enterprise Pain

An assessment of the data breaches that crop up like weeds each year supports the conclusion that companies, absent data governance, wind up building security architectures strictly from a technical perspective.



Here's one example of how a company that shares its users' data with others could connect the dots to sustain a data-safe business model. It starts with a data governance strategy that sets security and privacy limits about what data can be exposed to other entities and how: Customer information can be shared only after IT reviews and risk-analyzes the enterprise architecture to understand the data's sensitivity, locations and linkage points. That way, IT can pinpoint vulnerabilities, such as gaps in data encryption or anonymization, and set up sanitation layers that limit third-party access across all of its enterprise systems only to authorized and sanitized data, thus protecting against mishandling or other vulnerabilities.

Given that any company has in its possession important information about and relationships with people based on the private data they provide, every business should be keen to more intelligently and better understand related risks and protect against them under the banner of data governance—and avoid the costs and reputation damage that data breaches can inflict. That's especially true as the data-driven enterprise momentum grows along with self-service analytics that enable users to have greater access to information, often using it without IT's knowledge.

Indeed, with nearly everyone in the enterprise involved either in maintaining or using the company's data, it only makes sense that both business and IT begin to work together to discover, understand, govern and socialize those assets. This should come as part of a data governance plan that emphasizes making all stakeholders responsible not only for enhancing data for business benefit, but also for reducing the risks that unfettered access to and use of it can pose.

When all parties are alert to the need to pay close attention to data elements and inventory, and when the business embraces the idea of understanding data across the enterprise architecture and knowing how it feeds into operational business processes, it becomes possible to take a granular, offensive approach to securing and privatizing sensitive data. Finally, the dots will be connected.

Getting a Handle on Data Governance Requirements

Multiple components must be considered to effectively tie together the data governance, security and privacy trinity.

They are brought together as links in a data intelligence chain by:

CREATING ENTERPRISE MODELS

Enterprise models are the key to metadata harvesting and defining the data standards required for governance, translating technical formats to metadata-rich graphical models in a central repository. They offer a way of visualizing data assets across relational, cloud, Big Data and NoSQL platforms. An enterprise architecture function enables organizations to follow connections among data elements, wherever they are stored, to understand vulnerability paths and protect against security and privacy threats. Business process analysis informed by data governance standards delivers an extended view of data in context, so the organization can create policies for authorizing or limiting access to data.

BUILDING DATA CATALOGS

Catalogs are the foundation upon which to perform data governance and management tasks. With enterprise models defined, the work of automatically and continuously accumulating metadata from all data sources begins. Integrated, managed and categorized data fills a unified data catalog that cites data location, usage information and cross-domain relationships. Source-to-target data mapping integrates and synchronizes data, including data-in-motion, as it traverses through its lifecycle. Defined data profiles ensure that only controlled and high-quality data is deployed for digital transformation efforts such as data warehouse modernization.

INCREASING DATA LITERACY

Stakeholders, from data stewards to business owners and users, need a standardized and common understanding of what data terms mean within the context of the business. They also need the ability to easily find data elements associated with their roles, so they can produce trusted, data-driven insights. Being fluent in the business language of data helps in the application of business policies to ensure the desired outcomes, such as regulatory compliance.

Changing How the Enterprise Works with Data

With all these pieces in place, an enterprise has greater insight into the risks posed by lax or nonexistent data governance practices.

Such insight is the first step on the path to stopping the compromise of customer or even employee personal data or corporate intellectual property along any link of the data intelligence chain and every site where data resides.

It sets the stage to strengthen the policies, procedures and systems in pursuit of the big picture—that is, creating a cohesive triad of data governance, security and privacy. The comprehensive visibility that comes with bringing together the relationship an organization has built among data governance, security and privacy smooths the way for IT to determine what data is at high risk—perhaps unexpectedly so. That may be the impetus for re-evaluating existing auditing and reporting processes to more regularly identify activity that doesn't comply with data governance policies or putting more security and privacy controls around critical data sets.

Technology, for instance, may be used to revoke access to certain data by certain individuals as a result of better understanding these assets. Enterprise models show what data exists and where, what purposes it serves, and how it is structured and accessed so it can be appropriately governed in terms of security and privacy.

Of course, businesses must also take into consideration that, even with a three-legged data ecosystem in place, employees sometimes look for ways to circumvent rules and restrictions. While entities beyond the four walls of the enterprise certainly can and do infiltrate private data, risks also may be created by those within the business. Many of these are unintentional, as when individuals copy confidential data to a laptop to take on vacation with them—and then the laptop gets stolen. Changing the culture of the organization can help here, with chief data officers or those in similar roles continually reinforcing the message that data governance is everyone's business and that casual ways of treating information can lead to serious breaches.

CONSUMER VIEWPOINTS

69%: Percentage of consumers who believe companies are vulnerable to hacks and cyberattacks.

25%: Percentage of respondents who believe most companies handle their sensitive personal data responsibly.

87%: Percentage of consumers who say they will take their business elsewhere if they don't trust a company is handling their data responsibly.

PwC Consumer Intelligence Series

Common Data Targets of Cyberattacks

- Internal data: Operations, salaries, R&D
- Intellectual property: Top-secret projects, formulas, plans or other kinds of private data
- Client and customer information: Organizational clients, what services they buy, what they pay for them
- Marketing and competitive intelligence: Short- and long-range marketing goals and competitor knowledge

VIllanova University

Build the Data Trinity with erwin

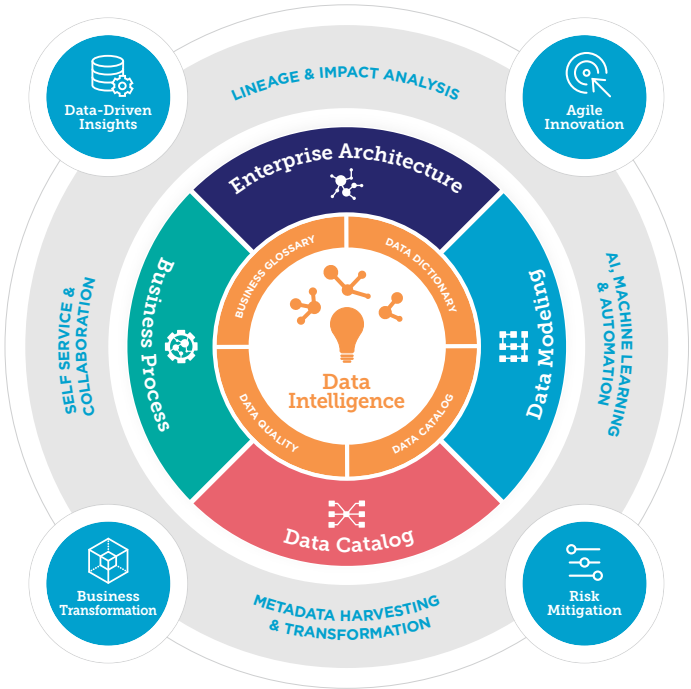
The erwin Data Intelligence Suite, consisting of erwin Data Catalog and erwin Data Literacy, underpins the entire data governance practice.

Together, these tools provide a better way for the organization to understand data within a business context, refine it for governance purposes, and get more value from it.

When an organization knows what data it has, it can define that data's business purpose. And knowing the business purpose translates into actively governing personal data against potential privacy and security violations.

With erwin Data Intelligence, data privacy and compliance officers can gain an unfettered view of where sensitive data resides. From there, they can seamlessly apply privacy rules to manage it, determine encryption requirements, and create access privileges to enhance risk management. They know better than anyone the consequences of carelessness when it comes to PII.

erwin's unique data intelligence offering is part of the erwin EDGE software platform that provides organizations with a complete and contextual depiction of the entire metadata landscape. No other vendor can automatically harvest, transform and feed metadata from operational processes, business applications and data models into a central data catalog and then make it accessible and understandable within the context of role-based views. Our ability to integrate and continuously refresh metadata from an organization's entire data ecosystem, including business processes, enterprise architecture and data architecture, forms the foundation for enterprise-wide data discovery, literacy, governance and strategic usage.



The erwin EDGE serves both technical and business users by providing them with role-based views of datasets from across the business, interdependencies across individual data elements, and a contextual understanding of how they are being used. Additionally, it creates an environment for IT and business stakeholders to collaboratively participate in driving data value—as well as protecting it to minimize risks.

No organization wants to be the next subject of negative headlines about a data breach. With erwin, businesses gain control over their information assets by activating the data trinity of governance, security and privacy.

The erwin EDGE supports the intersection between data governance, security and privacy by enabling an organization to:

- Manage any data from anywhere (Any²)
- Instill a culture of collaboration and organizational empowerment
- Create an integrated ecosystem for data governance that draws from one central repository and ensures data (including real-time changes) is consistent throughout the organization
- Break down silos between IT and the business by introducing a common data vocabulary, providing visibility across domains
- Mitigate a wide range of risks, including GDPR and CCPA compliance to cybersecurity threats.

Improve your organization's data governance, security and privacy. **Start with a demo of the erwin Data Intelligence Suite.**

About erwin, Inc

As the data governance company, erwin provides enterprise modeling, data cataloging and data literacy software to help customers discover, understand, govern and socialize their data to mitigate risks and realize results. The erwin EDGE platform facilitates IT and business collaboration in driving actionable insights, agile innovation, risk management and business transformation. We help government agencies, financial institutions, healthcare companies and other enterprises around the world unlock their potential by maximizing the security, quality and value of their data assets.

Connect with erwin at **erwin.com**

© 2019 erwin, Inc. All Rights Reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.