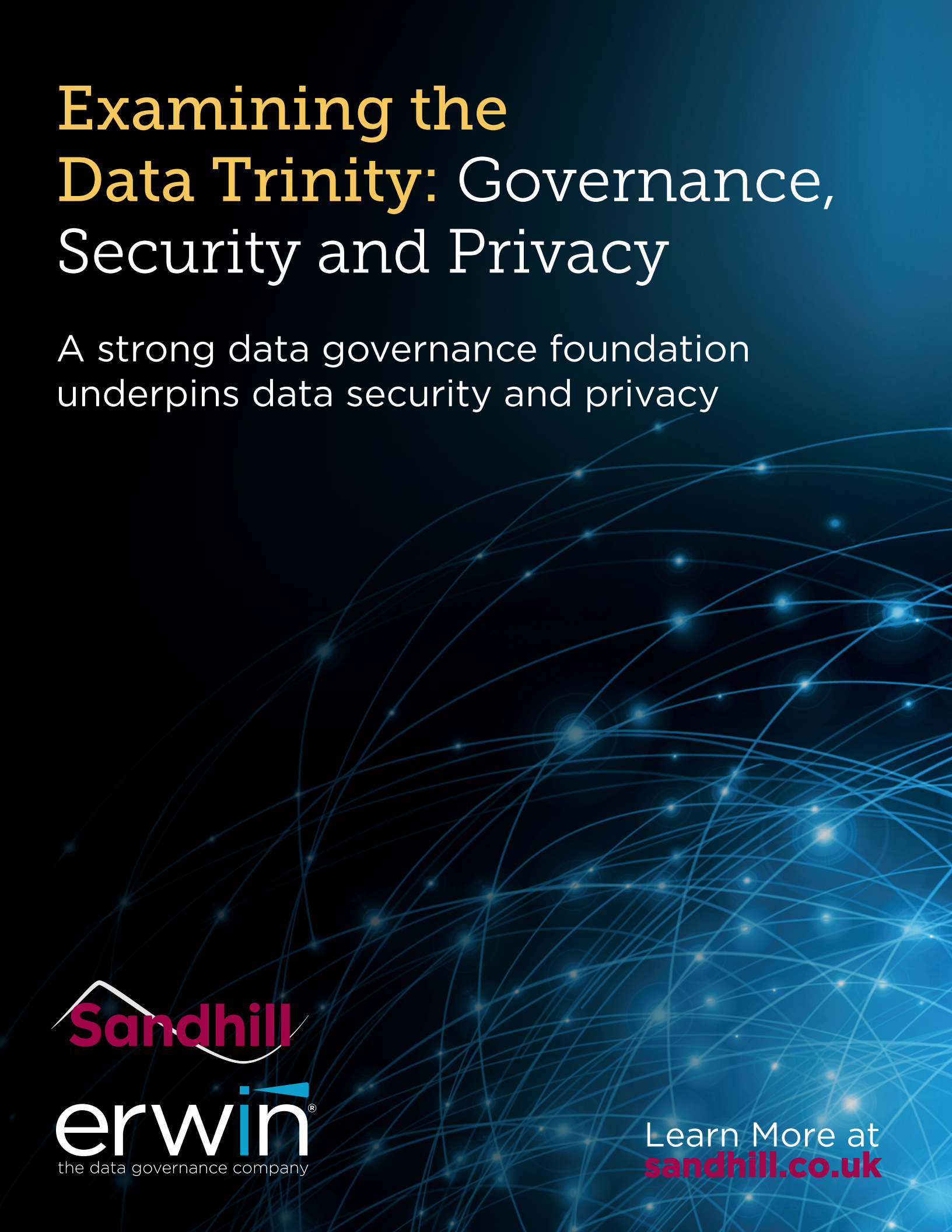
Examining the Data Trinity: Governance, Security and Privacy

A strong data governance foundation underpins data security and privacy



Sandhill

erwin®
the data governance company

Learn More at
sandhill.co.uk

Introduction

The news is awash with stories of companies whose IT security protections and controls failed to keep sensitive customer data private.

Facebook, Equifax, Uber and of course Yahoo immediately come to mind, but they're far from alone. In the last 12 months, businesses including Delta, Sonic and Whole Foods also disclosed they were victims of data breaches that may have jeopardized customer information. Media coverage of cracks in security 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. That knowledge is critical to supporting efforts to keep relevant data secure and private.

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.

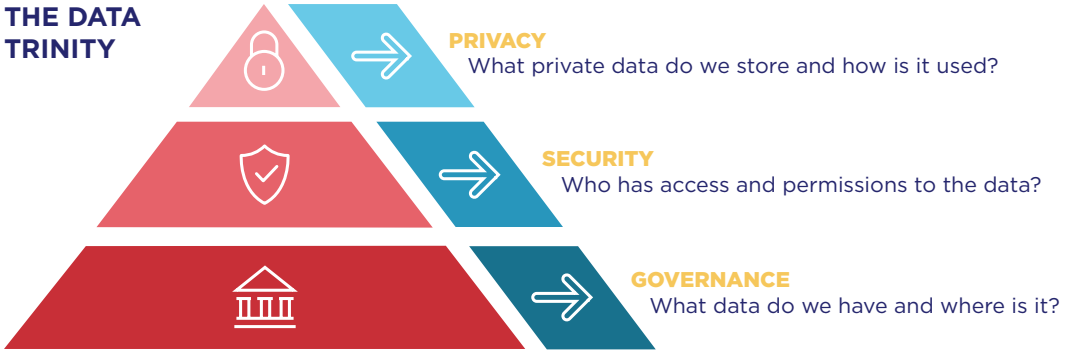
As a consequence, the private information held within organizations will continue to be at risk. Organizations suffering data breaches will be deprived of the benefits they had hoped to realize from the money spent on security technologies and the time invested in developing data privacy classifications. They also may face heavy fines and other financial consequences. For example, the U.S. Securities and Exchange Commission this year 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.

They don't gain visibility into the full data landscape—linkages, processes, people and so on—to propel more context-sensitive security architectures that can better assure expectations around user and corporate data privacy will be realized.

In sum, they lack the ability to connect the dots across the data trinity—governance, security and privacy—and to act accordingly.

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.

What's key to remember is that those components act as links in the data governance chain by making it possible to understand what data lives within the organization, its connection to the enterprise architecture and all the business processes it touches. Activating those components encompasses the following:

CREATE DATA MODELS

It's impossible to know what to do with data to privatize and secure it unless an organization knows what data exists and where, what purpose it serves, and how it is structured and accessed. Data models are the key to metadata harvesting and the means of defining the data standards required for data governance, translating technical formats to metadata-rich graphical models in a centralized repository. They offer a way of visualizing data assets across relational, cloud, Big Data and NoSQL platforms.

LEVERAGE ENTERPRISE ARCHITECTURE

Knowing how data that services the business relates to other data, whether stored on site or in the cloud, is more than just a value path for data analytics. The ability to understand and follow the connections among data elements also provides a way to understand vulnerability paths to protect against security and privacy threats. Data governance facilitates this through policies and standards around data movement, transformation and integration across systems.

CREATE BUSINESS PROCESS MODELS

Knowing what data flows across systems to understand where to place controls acts against sensitive information exposure. Data governance standards inform business process analysis for an extended view of data in context. This helps the organization comprehend whether and how to share data with internal parties, external partners, suppliers and so on, either providing authorizations for or imposing limitations on access.

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 IP along any link of the architecture and process 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. This will happen as the result of a better understanding of these assets thanks to data models imported into business process solutions that diagram and catalog workflows, and to enterprise architecture that maps corporate applications along with their associated data to specific business functions.

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

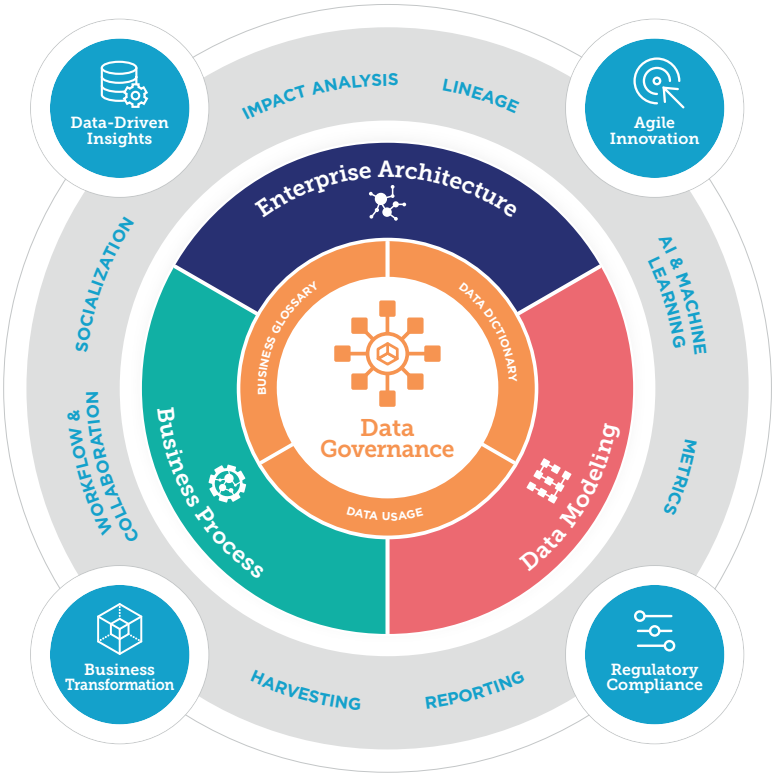
erwin's Enterprise Data Governance Experience (EDGE) is the means to understand what data exists and its context as it relates to processes, systems, organizational units and technology in use.

As the only unified software platform combining data governance, enterprise architecture, business process and data modeling—and applying each in accordance with its "any-squared" (Any^2) support for "any data" from "anywhere"—the erwin EDGE brings together all the components enabling organizations to ensure data security and privacy as part of an overall governance initiative.

Using erwin BP for analyzing business process models for information assets within business context can bring attention to security and privacy missteps. Using erwin EA for delivering complete enterprise visibility of data, applications and infrastructure offers the tools to inform and better prepare a data governance strategy underpinned by erwin DM for multi-source data discovery and analysis and erwin DG for describing, formulating, regulating and socializing data assets.

In addition to the EDGE being unique in providing both technical and business role-based views of datasets across the business, interdependencies across individual data elements, and a contextual understanding of how they are being used, it also provides the environment for IT and business stakeholders to collaboratively participate in driving data value—as well as assume accountability for minimizing data risks.

Within the erwin EDGE, the data trinity of governance, security and privacy gives businesses control over information assets. After all, no company wants to be the next subject of negative headlines about yet another data breach.



erwin EDGE: Supporting the Intersection Between Data Governance, Security and Privacy. It supports an organization's efforts to:

- Manage any data, anywhere (Any^2)
- Instill a culture of collaboration and organizational empowerment
- Introduce an integrated ecosystem for data management that draws from one central repository and ensures data (including real-time changes) is consistent throughout the organization
- Have visibility across domains by breaking down silos between business and IT and introducing a common data vocabulary
- Have regulatory peace of mind through mitigation of a wide range of risks, from GDPR to cybersecurity.

The **erwin EDGE Platform** will help you improve data security and privacy through integrated data governance. **Contact us to learn more.**

erwin, Inc. provides the only unified software platform combining data governance, enterprise architecture, business process and data modeling. Delivered as a SaaS solution, the erwin EDGE Platform unlocks data as a strategic asset so all enterprise stakeholders can discover, understand, govern and socialize data to mitigate risk, improve organizational performance, and accelerate growth. For more than 30 years, erwin has been the most trusted name in data modeling and its software foundational to mission-critical data programs in government agencies and leading financial institutions, retailers and healthcare companies around the world.

Connect with us at
sandhill.co.uk