Progress® DataDirect®

Six Practical Steps to Alleviate Data Security Anxiety

WHITEPAPER

Introduction: What is Data Security Anxiety, and What are the Impacts?

What is data security anxiety? Simply put, it is the manifestation of an uneasiness about the suitability of the existing data protection framework.

These anxieties are a result of not having adequate answers to the following:

- Can we protect against unauthorized data access?
- What undiscovered gaps are there in our organization's ability to harness the complexity of compliance with data privacy laws?
- Is the organization ensuring ethical and appropriate data use?
- What measure do we have to mitigate the exposure of sensitive corporate information?

As organizations rethink their data architectures while devising their cloud modernization strategies, data strategists must balance the need to expand access to corporate data assets for analytics purposes while ensuring compliance with a growing array of data privacy laws and standards. However, the desire to broaden data access exacerbates existing concerns about data security.

Traditional approaches are no longer seen as providing an adequate degree of protection. For example, implementing perimeter security around an on-premises data center is straightforward, and can protect against external attempts at breaching the firewall. However, digital transformation efforts that require the adoption of a multi-cloud hybrid data environment can significantly increase levels of "data security anxiety."

In this whitepaper, we describe the symptoms of data security anxiety and the concerns around ensuring a level of comfort as organizations rapidly adopt innovative distributed data environments that may span both on-premises and multi-cloud platforms. We will also suggest six steps for rethinking the requirements for data security and understanding ways to specify data protection policies and partnering more formally with vendors who align themselves with observance of data protection.

The six practical steps for providing a foundation for governed data protection - and alleviating data security anxiety

Step 1: Ensure Trust When Integrating New Software

The first symptom of data security anxiety is sudden chills that there are cyber vulnerabilities in your software stack.

Whether you are maintaining a software footprint solely on-premises or migrating your application stack to the cloud, introducing new software into the data and application environment is always fraught with risk. There is a reminder of these risks each time there are news reports about newly discovered vulnerabilities in both open-source and proprietary tools that are firmly entrenched in the software stack. This concern is magnified with tools and services that touch corporate data, especially data that is classified as sensitive or private.

There are many benefits to using open-source tools, but one must be particularly diligent in reviewing the source code to determine if there are any potential weak points that might allow malicious actors to infiltrate the enterprise application landscape. Organizations must also recognize that because many individuals may have their hands in open-source development, continuous code monitoring will be a necessity.

One can select technology vendors who are aware of these potential threat vectors and have instituted processes for ensuring against data exposure. These vendors have demonstrated compliance with required security standards and align themselves with the objectives of simplifying observance of requirements for appropriate data collection and management. Additionally, having integrated protections against violating legislative constraints such as opt-in/opt-out and data sovereignty.

This is particularly critical when working with connection drivers and data pipeline technologies. By partnering with vendors whose tools are engineered with data security in mind, your organization can increase the level of comfort in connecting to new data sources without opening new vectors of intrusion.

Step 2: Be Knowledgeable About Data Protection Policies

The second symptom of data security anxiety is feeling overwhelmed at the scope of rules and laws governing data protection.

Most organizations are likely to be familiar with at least one data privacy law such as the EU's General Data Protection Regulation (GDPR), or the state of California's Consumer Protection Act (CCPA). But data privacy rules are not new; there are already numerous laws and regulations on books imposing constraints on the use of private data. For example, in the United States, there is a long legacy of data privacy laws going as far back as 1974's Data Privacy Act. Worldwide, there are over 100 countries that have data protection legislation in place. All of that is combined with the continuously growing stream of new data privacy laws emanating from a variety of geopolitical jurisdictions.

An organization that is focused solely on complying with one data privacy law at a time is missing the forest for the trees. Trying to navigate compliance among numerous data privacy laws and other types of data protection directives is complicated. And when different privacy laws are introduced, providing varying definitions of what constitutes "personal" and "private" data, this complexity grows even further.

This symptom can be addressed by taking a holistic approach to understanding data privacy laws and corresponding protection policies. Instead of trying to deploy a collection of data protection rules for individual policies, consider developing a classification scheme and a taxonomy for sensitive data. By establishing taxonomies for articulating what is (and is not) defined as sensitive data within a defined data privacy law, you can directly link compliance with data security to each of the original source specifications.

For example, a driver's license may be considered private according to one jurisdiction's law but not another. By creating a tag indicating a data element's value is a driver's license, you classify the data element as potentially sensitive. But compliance is enforced in the context of who the data consumers are and how they access said data. This classification taxonomy provides a foundation for operationalizing data protection policy management.

Step 3: Catalog Your Data Assets

The third symptom of data security anxiety is a dread of exposure due to a lack of awareness of the organizational data inventory.

The growing popularity of data analytics, coupled with increased sophistication of data analysts and data scientists, has inspired many organizations to "democratize" their structured and unstructured data. Essentially, this means taking the data assets they have been hoarding for years, pushing them into a data lake, and enabling self-service access for the data consumer communities.

Despite the merits of data democratization, sharing ungoverned data creates a risk of exposing private business information that requires defense. Ensuring that sensitive information is accorded the appropriate level of oversight requires knowledge of what data assets exist and what sensitive information is contained therein. Without a comprehensive data landscape map, it is impossible to feel confident that organizational controls provide complete coverage of all potential vectors of exposure.

The root cause of this symptom is ignorance about data content. The remedy is to raise data awareness by surveying the data landscape, collecting intelligence about all internally sourced and externally acquired data assets that are being made accessible, and capturing that knowledge in a shareable data catalog.

Automated services can scan the content of each data asset to infer whether it includes potentially sensitive information. This inferencing can inform a categorization process that assigns classifications drawn from the data sensitivity taxonomy developed in accordance with the data protection policies. As a repository for collected knowledge about each data asset, the catalog informs consumers about the options they have for selecting appropriate sets for analysis.

Step 4: Understand Who Your Data Consumers Are

The fourth symptom of data security anxiety is ongoing fear of not being aware of who is accessing enterprise data and what assets are being accessed.

Concerns about external agents breaching your firewall and stealing data can be addressed by strengthening perimeter defenses. However, data leaks attributable to entities with allowed access to corporate data are grueling to find, whether deliberate

or not. In addition, to comply with data privacy laws, an organization must be capable of producing an auditable report demonstrating that sensitive data has not been inappropriately accessed.

Different staff members may be granted access privileges depending on the roles they play in relation to the business processes they support. Yet as the number of accessible data assets increases, it becomes increasingly difficult to effectively manage the assignment of privileges to each user.

Consequently, auditability can be informed through identifying and inventorying who the data consumers are and categorizing them according to their roles. Understanding which roles require access to the different types of sensitive data enables you to reduce the complexity of managing privileges. By aligning the roles with the classifications of data sensitivity, access privileges can be described in relation to the business process's requirements.

When an individual is assigned a role, that individual is automatically granted privileges to the data assets that role is allowed to access. When that individual changes roles, the previous privileges are removed, which in turn prevents unauthorized access. Following that, access logs can link each accessing user to that role, providing the desired auditability required for demonstrating compliance.

Step 5: Establish Data Protection Controls for the Appropriate Contexts

The fifth symptom of data security anxiety is the shock of recognizing that despite rules imposed by the different laws, rules, and regulations for preventing access, there are numerous instances where exceptions to those rules override the protections.

For example, consider that even though under GDPR a data subject can opt-out of allowing the data processor to use their personal data for one or more specific purposes, the law permits processing of personal data if it is necessary for compliance with a legal obligation or to protect the vital interests of the data subject. More to the point: Being uncompromising about data security may prevent your teams from accessing sensitive data under allowed circumstances.

Therefore, you can address this symptom by enumerating the contexts in which the data protection rules are overridden. For each externally defined set of directives (such as a data privacy law or an industry standard) that establishes classes of data sensitivity and imposes constraints on data access, document the specifics of any contexts that are relevant to exceptions to those constraints.

Examples include:

- **Location** - CCPA does not restrict selling a consumer's personal information if "every aspect of that commercial conduct takes place wholly outside of California."

- **Time** - Privacy laws absolutely prohibit the use of data of subjects below a certain age. That means that once that subject reaches the threshold age, the constraints about protecting that data may change.

- **Usage scenario** - Under GDPR, processing that touches personal data is permitted with it is necessary for the performance of a contract to which the data subject is a party.

Identify the conditions where accessing personal data is permissible and document how the data protection rules are modified in those situations. By describing the circumstances where there is flexibility in managing data security processes, you can reduce concerns that appropriate data accesses will not be flagged for noncompliance.

Step 6: Implement Policy-Driven Self Service

The sixth symptom of data security anxiety is the realization that too much data protection impedes benefitting from analytics.

A conservative approach in applying data protection guidelines will limit most data accesses, and this will result in preventing your data analysts, business analysts, senior managers, and data scientists from ever being able to analyze and review the results. Over-diligence in imposing security constraints diminish corporate agility in leveraging data assets for analytics and business intelligence.

Fortunately, our prior steps provide a framework for remedying this symptom. Recognize that a governed approach to data security will leverage the knowledge accumulated from

our other steps to produce a foundation for auditability of the data pipelines. Complying with data protection directives relies on creating a data security ontology that combines our three defined taxonomies: data sensitivity classifications, data consumer roles, and contexts for application of data security policies.

Organizations must enable self-service data access with governed controls configured according to the data security ontology. Data consumers playing specific roles will be able to access the data sensitivity classifications for which those roles are privileged within the bounds of the allowable contexts. This authorizes integrated monitoring and oversight of compliance with data security directives. Specifically, it enables monitor access, such as what data assets were touched, who requested access, what were the contexts, and whether any sensitive information was conveyed.

Considerations: Employing a Trustworthy Data Connectivity Solution

If you are suffering from data security anxiety, do not despair. While each of our six steps addresses one of the symptoms, together these steps provide a foundation for reliably ensuring compliance with data security and data protection directives. Yes, there is some effort involved in reading and interpreting data security directives and privacy laws to define the taxonomies and ontology that reflects the enterprise collection of data security policies. However, this effort will pay off when it simplifies the management of data security initiatives, as well as supports monitoring and auditability of compliance with data privacy laws.

Practically speaking, these steps must be implemented within and across the enterprise data fabric, and it is critical to acknowledge the role that trusted data connectivity solutions play. Knowing the risks of integrating modern technologies, one must partner with technology vendors that comply with defined security and data protection standards. In addition, work with technologies that are amenable to augmentation with policy-driven data access controls. Consider data fabric alternatives that enable integration with ontology-based and policy-based controls. This way, the enterprise will be properly protected against data security breaches and can capture the information needed to raise data awareness. Additionally, an organization will be enabled to simplify specification and management of data security policies and expand governed self-service to the different communities of data analysts, data scientists, and other data consumers.

About the Author

David Loshin, president of Knowledge Integrity, Inc., (www.knowledge-integrity.com), is a recognized thought leader and expert consultant in the areas of data management and business intelligence. David is a prolific author regarding business intelligence best practices as the author of numerous books and papers on data management, including Big Data Analytics: From Strategic Planning to Enterprise Integration with Tools, Techniques, NoSQL, and Graph and The Practitioner's Guide to Data Quality Improvement. David is a frequently invited speaker at conferences, web seminars, and sponsored websites and channels. David is also the Program Director for the Master of Information Management program at the University of Maryland's College of Information Studies.

Learn how Progress DataDirect's connectivity solutions can relieve your own data security anxieties.

About Progress

Dedicated to propelling business forward in a technology-driven world, Progress (Nasdaq: PRGS) helps businesses drive faster cycles of innovation, fuel momentum and accelerate their path to success. As the trusted provider of the best products to develop, deploy and manage high-impact applications, Progress enables customers to develop the applications and experiences they need, deploy where and how they want and manage it all safely and securely. Hundreds of thousands of enterprises, including 1,700 software companies and 3.5 million developers, depend on Progress to achieve their goals—with confidence. Learn more at www.progress.com

/progresssw
/progresssw
/progresssw
/progress-software

Progress