The Top 5 Data Security Risks for Data Driven Organizations

The Cloud Security Alliance (CSA) has consistently ranked data breaches as the number 1 threat facing cloud computing. A data breach occurs when sensitive or confidential information is accessed, viewed, or released by an unauthorized actor and includes "any kind of information that was not intended for public release, including—but not limited to—personal health information, financial information, personally identifiable information (PII), trade secrets and intellectual property" .

Data-driven organizations suffer from a heightened risk of data breaches. These entities rely heavily on data for decision-making, operations, and innovation, making the protection of data assets even more critical. The vast volumes of sensitive information they accumulate, including customer data, create a higher level of exposure to risks, and often at a scale and complexity that demands adherence to stringent regulations. Furthermore, the very nature of being data-driven means that more users and applications require access to data for informed decision-making. While this democratization of data is essential for agility and innovation, it simultaneously amplifies the risk of data exposure or misuse,

Here we will highlight the top 5 risks to data security we see enterprises facing as they become more data-driven.

1 Privilege, Privilege Escalation and Identity (ab)use

Privileged access, often granted to administrators and high-level users, holds the keys to sensitive data and critical systems. Failing to manage this access rigorously can result in unauthorized data breaches, insider threats, or even external attacks. Privilege escalation, traditionally through vulnerabilities associated from poor system hygiene, and in databases through misuse of application roles, allows theft of data by unprivileged users.

The importance of managing data access is particularly evident with "joiners, movers, leavers" (JML) within organizations. When new employees join, existing ones change roles, or individuals leave the company, their access privileges need to be swiftly adjusted. This is further compounded within business applications where toxic combinations of access (Toxic Access) could occur through the assignment of multiple roles or inappropriate rights which need to be managed accordingly (eg in payment applications - the same users shouldn’t have the ability to authorize an invoice for payment and pay the same invoice).

Technical teams often struggle with handling JML and Toxic Access across systems which aren’t integrated with a central identity manager (in other words, a lack of single sign-on or identity federation). While this has largely been solved for line of business applications by using technologies such as SAML, oAuth, and JWT, unfortunately 4 of the top 5 databases (as ranked by db-engines - https://db-engines.com/en/ranking) do not natively support such privilege management or federation.

Examples of privilege and identity abuse:

- ➤ Application developer accessing database using application service credentials
- ➤ Employees using borrowed credentials for speed of access
- ➤ Bad actors stealing long lived credentials

2 Data Exfiltration

Once an actor has access to an organization's sensitive data, there’s two primary malicious patterns we see: infecting the organization with ransomware, or exfiltrating the data.

Structured data does not lend itself to typical ransomware techniques. Rather, the primary objective of bad actors is the exfiltration of data, usually to later demand payment from the organization for "its deletion", or blackmail their target with the threat of public release. While this is aimed at causing reputational damage, it can also have significant legal and regulatory consequences for the organization.

Even the best staffed security teams, if they've been able to build processes to ensure privileges and identities are managed properly, grapple with implementing the principle of least privilege for applications and databases. Often, this results in the creation and management of roles, and an attempt to assign granular permissions to roles. With databases in particular while they allow privilege grants at the table/view level, there is no way to deploy protections at the database level for privileged (DBA / root type) accounts, a lack of methods to constrain the volume of data (rows) which can be returned by a query, and limited capability to mask or obfuscate data.

3 Misconfigurations and Change Control

Misconfigurations and inadequate change management processes represent significant threats to data security. Misconfigurations in software, systems, or cloud infrastructure can unintentionally expose sensitive data to external threats. On the other hand, improper change management processes can result in unauthorized modifications to security settings, inadvertently providing access to unauthorized users or malicious actors.

In a traditional (data center + corporate network) model, the likelihood for abuse was mitigated by other controls such as ingress firewalls, VLANs, and VPNs. While almost all cloud platforms provide robust and granular security controls, they all provide a high degree of autonomy to the platform users which significantly increases the scope (and risks) of misconfigurations and makes change management more challenging.

Examples of data exfiltration tactics that bypass network and appsec controls:

➤ Privileged users doing full table scans

➤ Business users exporting BI tool reports to local files

➤ Misuse of application privileges by internal users

4 Limited Visibility

Visibility is paramount in preventing data breaches. Without a clear understanding of what is happening within an organization's data environment, it's nearly impossible to detect, respond to, and mitigate potential threats effectively.

For structured data, this visibility falls into the following three categories:

1. Where does sensitive data reside?
2. Who has access to that data?
3. Who consumed specific records?

These questions, specifically #2 and #3, get hard to answer at scale because conventional IAM services don’t provide controls at the granularity of (types of) records. As the amount of data being used and the number of channels from which it is consumed increases, an organization’s ability to answer these questions decreases.

5 Insider Threats

Within data-driven organizations, insider threats get particularly complex because of the vast data ecosystems they operate in, often consisting of a large number of users accessing data through visualization tools (such as Tableau) that share a single role across those users. Any malicious actions can be stealthy and difficult to detect.

The “insider threat” was traditionally used to imply someone within the organization would be the originator of an incident. However, given the prevalence and reliability of boundary controls (eg: firewalls) bad actors often use techniques to compromise internal user’s devices and abuse their access. Security teams mitigate typically against this risk using MFA and a just-in-time access model.

With databases and data lakes this becomes a particularly egregious risk because of the long lived credentials and the lack of MFA capabilities.

Types of insider threats:

- Malicious insiders with access to sensitive data
- Curious employees poking around
- Third parties with access to data
- Ex-employees with unrevoked access
- Security policy evaders who circumvent controls to speed up their work

About

Cyral provides controls for privacy, compliance, governance and protection thereby reducing risk, complexity, and cost for managing structured data. The Cyral platform discovers data, unifies access controls for users and applications, enables fine-grained authorization policies and provides complete monitoring and reporting. This comprehensive coverage enables risk-based governance, limits the blast radius of data-related incidents and reduces overhead and costs. Cyral's technology allows customers to implement data security controls using their existing, centralized entitlements, thereby simplifying administration and automating remediation. Customers use Cyral to accomplish least privilege, data minimization, spillage prevention and Zero Trust.

For more information, visit **www.cyral.com** or follow **@CyralInc** on X.