SailPoint

WHITE PAPER

# Changing the Game with **Data Access Governance**

Each year, organizations face an ever-mounting threat of hackers and other hostile entities that aim to breach companies in order to gain access to their systems and data. In fact, targeted attacks have nearly doubled since 2013. While organizations are working overtime to address the risks and become more secure, more issues seemingly crop up every day.

The impact of these rampant data breaches reaches far and wide and unstructured data factors into an organization's risk. But there are challenges associated with securing and controlling access to that data; knowing how you are at risk isn't enough to protect you without a game plan. You can better secure your organization by integrating your data access governance plan into your overall identity strategy. That is, governing your data by looking at who can access your data, as well as what they are doing with it.

## The Impact of Data Breaches

It seems as if it occurs every day: another enterprise has been breached. Its data has been taken, its secrets revealed and the consequences can be astronomical. When Orange Telecom in France was twice breached in 2014, over 1.8 million customer records were stolen. Names, email addresses, phone numbers and birthdates were all among the information stolen, all of which could easily be used to conduct phishing scams on those affected. While it's scary enough just thinking of what would happen if it were your organization that were breached, it's important to understand there's more at stake than you initially realize.

- **Direct financial costs:** Perhaps the most well-known and well-publicized fact is that data breaches are expensive. But it's not just the regulatory fines and the compensation to customers whose information was leaked. After a company experiences a breach, it's not unheard of for their liability insurance rate to skyrocket by 200 – 400%.

- **Trust/Reputation damage:** News outlets have field days when data breaches occur, especially when the organization involved has a highly recognizable (or, in the case of Ashley Madison, controversial) brand name. Even without having to deal with such a PR nightmare, data breaches can lead to loss of trust with customers which, in many cases, is irreparable.

- **Increased audit requirements:** After a breach, it's normal to see a significant increase in the audit requirements placed on a firm, both internally and externally. This increase can last for years, increasing the time and cost associated with managing and validating your security controls.

## Unstructured Data is the Next Frontier

Only addressing portions of your enterprise's IT environment is no longer enough; you simply cannot afford to only secure and control access needs to structured systems. It's not just the traditional applications and systems that are vulnerable to attack, either. Systems that hold unstructured data (email servers, file shares, cloud storage applications, etc.) must be part of your overall plan.

Unlike information stored in structured systems – which can be managed using standard identity governance approaches – unstructured data exists in many different formats and locations, and with this complexity there come challenges to both controlling and governing access to this type of data.

Securing the enterprise means managing structured and unstructured data access by all users through all apps.

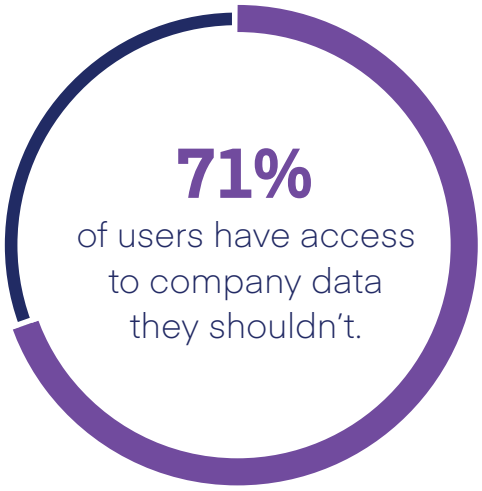
## Understanding the Challenges of Unstructured Data

Securing access to unstructured data is a challenge for any enterprise, and it can be categorized into two general parts: how to control access, and how to govern those controls.

### Controlling Access

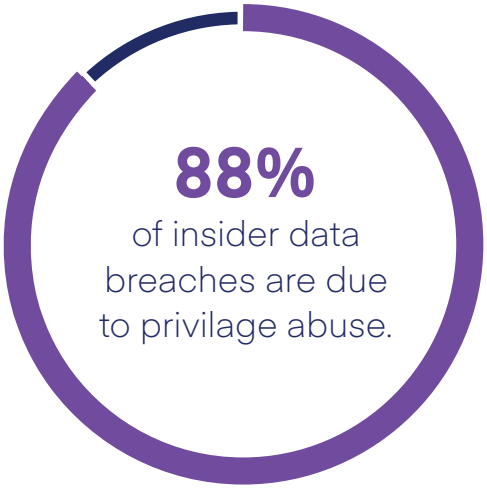
The first challenge, controlling access, lies in three parts: for any organization there are numerous places where this data is held, and there is little oversight during creation, modification or deletion of data.

- The myriad of places in which organizations keep their data is growing with each passing year. Microsoft SharePoint, Dropbox, Office 365, Exchange, intranets, file systems, etc. all contain unstructured data that becomes increasingly difficult to manage as more data is collected and more systems are added. These systems are both on-premises and in the cloud, with combinations that are usually unique to the organization, making a "one size fits all" approach impossible.




- With unstructured data, the users are in charge, not IT. While structured systems may have a data architect designing an access model to protect sensitive information, most unstructured data systems let individual users create, modify and delete existing data without requiring formal approval. This allows for users to largely control where data is kept; often, users don't think about the security risks involved in creating data and placing it in a convenient, albeit insecure location.

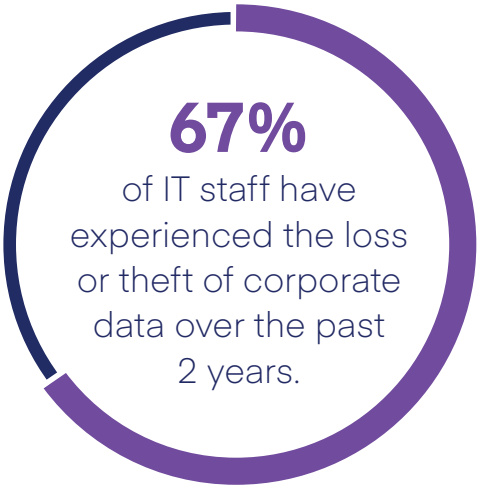
- Sometimes, in an attempt to address many of the gaps created by the first two issues, IT implements access control models that add to the complexity of securing unstructured data. Because access to unstructured data is often managed using group memberships to simplify administration, this approach can create blind spots as to who really has access to sensitive data.




**Governing Controls**

The second challenge of unstructured data – governing the access controls – also has three parts: enterprise-wide visibility into what data exists, regular reviews of data access and unequal controls for unstructured and structured data in relation to audits.

- In most organizations, holistic "maps" simply don't exist of what type of unstructured data lies where. This is further complicated by needing to know three different pieces of information about that data: "What data exists?," "Where is it?," and "Is it sensitive?" Without the answers to those three questions, it's impossible to effectively manage both the data and who has access to it.
- Answering the "who has access to what" question is something every organization needs to be able to do whenever it is asked. And while most organizations have systems in place to assist, most unstructured systems reside outside those processes. This makes regular review of employees' access nearly impossible. Combine this with the usual lack of understanding where data exists, and a significant security risk comes to light.
- Much like with the other facets of the challenges concerning unstructured data, the key to being secure is acting holistically. This is, of course, true for your audits. The number of material deficiencies related to securing access to unstructured data has skyrocketed in the past few years.




## Changing the Game by Extending Identity to Unstructured Data

Once you understand the challenges associated with governing unstructured data, you can begin to build a game plan for securing it – and your organization. In this world, data is the starting point for everything you do, though it's not the total picture. People are the other variable. At the end of the day, your goal is to keep your data secure while allowing the necessary people use it for business objectives. Fortunately, all access to data can be tied to an identity.

What connects the two dots of data and people is access. In this case, data access governance applies the same principles we've used in identity governance by linking data to people through a visible and well-structured access model. Only after performing the following important activities concerning your data, people and their connecting access can you build a data access governance program that will work for your organization.

## Data

In order to implement a strong data access governance strategy, you must start with the data itself.

1. **Where is your data?** To ensure you have all the information you need to create a secure system, you must first know where your data lives. This usually includes interviewing the data application owners to understand what kind of data they use, and where they usually store that data. Recruiting the help of tools can speed the process along by scanning your typical unstructured data repositories: email systems, file shares and collaborative portals, in addition to your cloud applications such as Dropbox and Office 365.

2. **What is your data?** Once you know where all your data resides, you can then categorize it based on the type of information it actually contains. This is especially important to identify where your most sensitive data is located so that you can focus your efforts on the areas of highest risk. Intellectual property files, customer/employee information and other types of information present your highest security risk; categorizing your data by type will make it easier to manage and improve security.

3. **Is your data in the right place?** The last step, once you know where your data is and what it contains, is to determine if it was placed in the correct location. Often, users place data in a convenient spot, but that may leave it in a vulnerable place. Identifying if this combination is correct is a critical part of your overall strategy; when you combine overexposure (data that is stored in a location where the wrong people have access) with sensitive data, you end up in a high risk situation. Once data is located in the correct place, it is much easier to manage and secure.

**CASE IN POINT:**

### Sony Pictures

When Sony Pictures was breached, it was found that employees' account names and passwords were being stored in Word, PDF and Excel files. Even privileged accounts and passwords ended up being exposed as part of the process. Because this sensitive data was being stored in an insecure location, this toxic combination led to a more extensive breach than what we might've seen had these documents been properly secured.

## People (Identity)

After locating, categorizing and verifying your data, you need to take a look at the people who have access to the data.

1. **Who are your users?** Just as it is important to know what data you have, you also need to understand who your users are. Employees, contractors, vendors, business partners and other users may have access to your unstructured data systems and will use and access data in different ways.

2. **Who uses your data?** The reality is that data stewardship is an important part of securing sensitive data assets. Too many users simply assume the data they create and use is safe because it is housed on organizational systems and applications. Additionally, it is common to find a laissez faire attitude towards protecting access to sensitive information and rather save the data wherever it is most convenient. Finding who uses the data in your enterprise is important in order to change processes and secure your data, and it's also a critical part of the next step .

3. **Who are your data owners?** In addition to finding who manages the data in your organization, it's necessary to designate concrete data owners for that information. Data owners become the first line of defense in securing and managing access to data. Because they can feel personally responsible, they actively ensure that data is in the right location and only accessible to the right users. Finding these owners can, of course, take some time and may be a frustrating process. Utilizing the user community and "crowdsourcing" the owner election process can significantly reduce the time taken and improve your chances of finding the most appropriate owners.

## Access

Once your data and your people have been identified and understood, it's time to connect them with access.

1. **Who has access to what?** The first step is to pair data and people to determine who has access to what, and you must first focus on the most sensitive data. Remember, this is also impacted by the data collected when modeling your users and defining their relationships with the enterprise. Identifying the pertinent information for your most at-risk areas will help to guide you as you work through the whole of your unstructured data.

2. **How is access granted?** Most of the fundamental issues with how your users access your data is found when establishing how access is granted in your organization. During this process, many of the challenges discussed earlier will come to light. And while this step starts with understanding whether access is granted directly or indirectly, it may result in needing to fix issues within the access models to improve security.

3. **How is access validated?** No program is complete without ensuring its future success. Cleaning up permissions, finding overexposed data and fixing other issues that arise during this process is a great boon for your organization, but it's very easy to fall back into the processes that left you insecure in the first place. Setting up regular access reviews, as well as establishing appropriate access patterns and methods for detecting anomalous or inappropriate behavior can help safeguard enterprises against potential security risks. The earlier these types of issues can be detected, the more quickly you can employ risk mitigation strategies and potentially limit the damages from (or perhaps even prevent) a breach.

## Summary

Organizations today face more threats than ever before, but luckily, the tools to help them secure their current and future assets have evolved as well. While IT teams already have a number of daunting challenges facing them, data governance is an important part of securing the lifeblood of the enterprise. Holistically knowing where data is located (whether it's structured or unstructured), who has access to what data and how they are using it can help to detect problems, mitigate risk and secure your organization.

The future doesn't have to be bleak; move your organization to a paradigm that allows IT security teams to manage all data access through a common set of tools and processes. Have all the information on which to base your decisions and employ the basic tenets of protecting your data. Combined with your identity governance framework, you can ensure a more secure and stable enterprise.



WP1009-1710