
# Do You Know

# Who Owns Your Data?

SailPoint

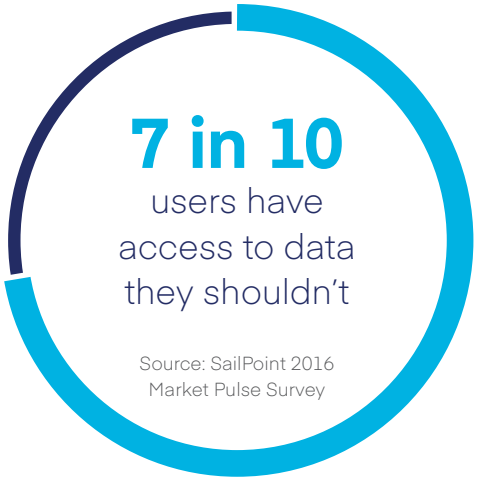
Managing access to enterprise applications and data has changed in the past few years as data breaches have become increasingly more frequent and pervasive events. Organizations must understand that their data is not safe from being the target of an attack, and hackers have slowly but surely transitioned to attacking the human vector: an organization's users. Its identities.

But the threat of a data breach should not be the only spur to secure access to an organization's data. While the inevitability of an attempted data breach – if not a successful one – is nearly certain, organizations must learn to instead focus on what they can do once they are well-prepared for a breach. And it all starts with unstructured data.

## Governing Unstructured Data is a Growing Problem

Unstructured data is growing in volume – exponentially in most cases. Every e-mail sent or document created adds to the number of files organizations have. Meanwhile, identification and classification has become increasingly more difficult. PDFs stored in a cloud storage application may contain innocuous office party planning memos, or they may contain sensitive healthcare patient information.

Even organizations who have already established tight controls over access to sensitive systems and applications are not immune to this growing problem. Take into consideration an employee who has appropriate and authorized access to the organization's financial systems can export data into a report. This can then be easily shared with others and stored not only in one location but as time goes on and is shared again and again, it propagates and is completely outside the organization's view.




Because unstructured data resides outside of traditional, structured systems such as applications and databases, and generally does not have an easily identifiable owner overseeing who has access, ensuring that sensitive data is secure can be a tall order.

One challenge with how organizations secure their unstructured data is due to a lack of predictable data owners. Structured systems such as SAP typically have a business owner to oversee the application and govern who access to it. But in most organizations, there is no complementary owner for the unstructured data stored in files. Instead, the caretaking of unstructured data is usually left up to the users who create or use it on a regular basis. In most cases, this is not the best steward of the data to ensure its security.

In order for an organization's data to be protected, access to it must be governed. Without proper data owners, unstructured data in files can be easily overlooked, incorrectly classified and improperly managed in terms of who has access and where the data is stored.

Organizations who fail to actively assign accountability to data owners for understanding who should have access and who does have access to sensitive data in the enterprise are leaving themselves open to data breaches and regulatory penalties.

## Electing the Right Data Owners

Legacy approaches attempt to determine data owners simply based on their usage of the data. Unfortunately, this leads to ineffective mapping and often causes more problems than it solves. Imagine a team member in who is creating the blueprints for a new product design and storing them in cloud storage for easy distribution. Under legacy tools, he would be assigned as the owner of these files. However, he may or may not know who else should have access to these files or the others in the folder in which he is creating the PDFs. More than likely, his supervisor or a lead product manager should be the one that owns the data and should govern who has access to it, even though he/she may access it on a much less frequent basis than the original team member.

Instead of assigning data owners based on usage, your process should allow for business users to give direct feedback or elect an owner for sensitive data. The issue many organizations face is that the correct data owner cannot be found by traditional means; more often than not, this information only resides in the minds of the users who actively utilize the data. The solution? Rather than attempting to create rules to automatically assign owners, ask those who work with the data on a regular basis to be your eyes and ears. Those who work most closely with the information can collectively identify who would be best to own and govern access to the data in question.

As the amount of unstructured data in an organization grows, so does the complexity of ensuring the right people have the right access. While automated methods of finding, categorizing and controlling access to the data can be a good start to mitigating risks, ultimately the ability to identify the proper business owner for your unstructured data is the only way to truly protect it.

By extending an identity governance implementation to manage data access, many processes can also be automated to expedite access certifications and feed information to your identity governance solution. When IT has all the information on an organization's users and their access – to both applications and data – they have the power to quickly make the right decisions in the event of a data breach.

**SAILPOINT: THE POWER OF IDENTITY™**

**sailpoint.com**

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.



EB1030-1709