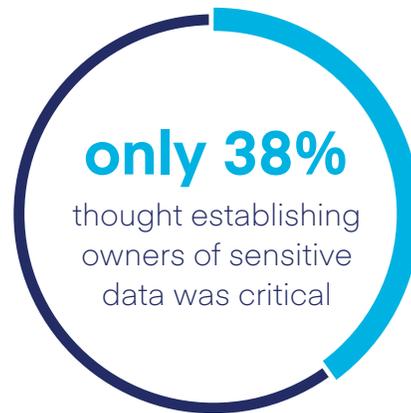# Protecting Access to Enterprise Data

SailPoint

Enterprise data needs protection. Intellectual property. Financial records. Employee and customer personal data. This type of data is what hackers want to get their hands on. The important-to-a-company data. The data that's worth money or is damaging in some way to the enterprise. And hackers know the easiest way to get to that data is by exploiting the human element of an enterprise.

While organizations have shored up their technical defenses and strengthened the proverbial walls around themselves, one weak link is still as vulnerable as ever: people. We inherently trust when perhaps we shouldn't. So when an e-mail comes through with the "CEO" asking for the latest quarter financial report or a copy of the blueprints for a new product, we tend to do what's asked of us.

Because users are who hold the keys to accessing the sensitive data at the enterprise, and they are the attack vector of choice for hackers, it only makes sense that IT security should revolve around them. But, in a recent survey conducted by SailPoint, we found that less than half of our identity-savvy respondents viewed certifying user access to sensitive data as a critical function toward minimizing security breaches.

Just as concerning was that only a little more than a third of respondents believed it's critical to establish (and know) owners of sensitive data. Without these two key aspects of an identity governance program, organizations are at a higher risk than ever for the inevitable data breach.

only 48%
thought certifying user access to sensitive data was critical

only 38%
thought establishing owners of sensitive data was critical

Secure the Human Element

In order to protect our enterprise data, we have to secure the identities in our enterprise. They are who access and use corporate data on a regular basis. The point where many enterprises lack the proper controls is with access to unstructured data. Structured systems, such as SAP and Oracle, are usually assigned owners and are strictly maintained. But unstructured data stores, such as SharePoint or e-mail

servers, may not have the same oversight. With Gartner estimating unstructured data to be 80% of all enterprise data, this is not a small problem.

But it is a solvable one. Extend traditional identity governance processes to how you manage access to sensitive data. Automatic, periodic access certification assures that users have the right access to the right data at the right time. Electing proper data owners keeps data healthy and ensures access requests are granted and rejected appropriately. You can then further expand your identity governance program to include forensic data classification and role management, among other security aspects, to even further protect your sensitive data.

The Power of Knowledge

The fact of the matter is you can't protect what you can't see. But when IT has full visibility: who has access to what, what they're doing with that access – all regardless of whether the data is in structured or unstructured stores or if it's stored on-premises or in the cloud – the enterprise has the power to protect the sensitive data they need to keep safe.

Regular re-certifications ensure there is no errant access from terminations or lateral employee movement. Data owners who were chosen because of their familiarity with their data know, at any time, who should have access to what data and can keep that data healthy and well-maintained. With a robust identity governance program in place, containing these two key aspects, you can be confident that your identities are only accessing the data they need to perform their jobs.

With this knowledge, your organization is empowered to be confident that access to your data is secure. This allows you to chase new opportunities and do what you set out to do in the first place: grow your business.