stealthbits
NOW PART OF netwrix

WHITE PAPER

3 STEPS TO GETTING DATA ACCESS GOVERNANCE OFF YOUR TO-DO LIST

TABLE OF CONTENTS

INTRODUCTION

If you are like me, there are many things you can check off your to-do list every day. However, if you are really like me, then there are some things which seem to lurk on the outside of your productive daily routines. These items are not always little matters, either. Sometimes they get forced out of view specifically because they are enormous, time consuming tasks which are much less satisfying than knocking over whole armies of short term goals. The way to tackle these daunting tasks is to break them down into more manageable pieces which can be achieved.

> **There are huge piles of data on file systems, file shares, and collaboration systems like SharePoint which are all but unknown to the security world.**

Data Access Governance (DAG) is security's big unaddressed to-do item. There are huge piles of data on file systems, file shares, and collaboration systems like SharePoint which are all but unknown to the security world. Though every time I ask about Data Access Governance, every single security professional – and everyone else in IT for that matter – will freely admit that they knew there was a problem there. DAG has been that to-do item IT security has had for years, but they just kept pushing it aside for other goals. Today, however, there are strategies which can make DAG more approachable. We are going to break DAG down into 3 steps that you can use to finally check this big one off your list.

3 THINGS YOU CAN DO TO TACKLE DAG

If the description of how big this problem can be did not send you off screaming, congratulations on having the fortitude to make it this far. What we are going to attempt now is to get a real understanding of how the DAG problem might be solved, in part. I say "in part" because we are going to discuss part of the DAG healthy breakfast. These are technology approaches that can help you get the problem under control.

However, like every real security issue, the whole healthy meal would include process reform, new controls, and other business side reforms to ensure the problem does not get out of control again. So you can consider this a great starting point which will help you clean and organize the current environment. It is also worthwhile to note that I cannot claim this advice as my own.

We at STEALTHbits have learned this from our clients. While we have been providing the technology to make things work, they have been the ones who taught us how they realistically approached these problems and achieved measureable success. The three steps they have shown us are:

1. Get open shares under control.
2. Find, classify, and identify owners for your sensitive data.
3. Run an access certification program to align access to business needs.

Get Open Shares Under Control

Open shares are like kryptonite for security models. Even the best security is powerless in the face of a file share that anyone can write to. The worst part is that sometimes an open share does make sense. There are some files that everyone does need access to – things that are distributed by HR about benefits, for example. Does everyone really need write access to that sort of share? Maybe you have people taking interactive PDF files, filling them out, and then saving them back to the share. So your answer is "yes, they do need write access." (That goes back to that business process part of the healthy breakfast.)

If your network is like so many others we have seen, then there are likely lots of shares with access granted to high risk trustees like AD's "Authenticated Users". How did they get that way? At some point in time, someone with enough clout asked someone in IT with just enough privilege to do it, and they did. That is the most common scenario. The last effect is a conduit for data of all kinds which needs to be shut down, or at least locked-down better than it is. Luckily, this is an easy problem to address once you have the will. Shares can be scanned, the people who have access analyzed, ownership determined through heuristics, and then the access can be lessened in scope to where it makes sense.

At some point in time, someone with enough clout asked someone in IT with just enough privilege to do it, and they did.

Figure Out Where Your Sensitive Data Is And Who Owns It

The open shares are a burning fire, and that is why you go after them first. When the smoke clears, there will still be a lot of data that needs your attention. The key question is where to start. That is why the next step is figuring out where your sensitive data lives. Which begs the question: what data is sensitive? This is another question that will vary for everyone reading this (unless you are reading it over a colleague's shoulder for some odd reason).

- Is your organization regulated?
- Do you handle credit card data and need to worry about PCI?
- Are you publically traded and under SOX controls?
- Do you need to worry about ITAR because you are in the military supply chain?
- All of the above?

It may seem impossible to answer "yes" to all of the above, but we have seen it. The definition of sensitive data will vary according your answers to these questions. However, that list is just the tip of the iceberg. Maybe your

The open shares are a burning fire, and that is why you go after them first. When the smoke clears, there will still be a lot of data that needs your attention.

organization has intellectual property in forms that can live in unstructured data (e.g. chemical formulas or complex processes) which you wish to protect from the eyes of the competition. That's sensitive data. Now when we return to the question about where to start, the answer is clear: you start where your sensitive data lives.

The first part of getting sensitive data under control: know what the sensitive data looks like. Sometimes that is easy. If you are worried about HIPAA or PCI, the rules are clear. You are looking for things like credit card numbers, social security numbers, and personal details. These are pieces of data that are well understood, and there are many proven ways to go out and find them in data. Things get a bit more complex with something like ITAR. ITAR says you have to control anything that may be used in the military supply chain. But how do you identify things like that? Most people we have seen go after part numbers and other identifying data. That means understanding those, locking down ways to find them, and also knowing which ones you need to look for.

The most complex piece is when you want to look for stuff that is sensitive from a pure business standpoint – your "secret formulas". Those are usually difficult to pin down to stable pattern to seek for and are more likely to be in many places you would not expect. Luckily, the easy part these days is the scanning, once you know what you need to look for. Solutions come out-of-the-box ready to handle the major regulatory conditions and give you flexible ways to create your own search criteria, including Optical Character Recognition (OCR) support to scan for text within images like medical records. Then when you have things to look for, set the technology loose on your network and let it find the places where you need to address security concerns the most.

Once you have located your sensitive data, you can classify it based on criteria that make sense for your organization; and assign risk levels such as restricted, confidential, and internal. These levels help you determine the best way to secure each type of sensitive data. Restricted data is the most sensitive. It contains information on your organization's intellectual property, financial health, and M&A, which could materially impact your business if exposed. Consequently, it needs to be highly protected. Confidential information is the next most risky and includes data on your customers, employees, and transactions. Confidential information has been the target of many recent attacks and also need to be protected. The last category, internal, is the least sensitive and comprises items like HR polices and organization charts.

Companies often go one step further by tagging sensitive data with descriptors like PCI or PHI, which become part of file properties. These tags can be scanned and read as part of ongoing governance controls and are helpful for maintaining an audit trail.

As you find your sensitive data and classify and tag it, you also need to have these scans sort out who owns the data. You are going to need to have those folks answer some questions for you. They will need to make sure that access to this data is best aligned to the business needs – the next step.

Run An Access Certification Program To Align Access To Business Needs

The sensitive data tells you where to start, but what are you starting? What needs to happen is a program where you get the only people who actually understand all this data to tell you who should actually be able to touch it. Who understands who should have access? Is it the dude on the help desk who has usually been asked to make these choices? No. The people who understand what access to the data ought to be are the people who created it in the first place – the business users.

What you are going to do now is get them into the game. They created all this data, and now it is time for them to sort it out. Before this becomes too much of an IT vs. the end user session, though, it is worthwhile to recall that it was not all the end user's fault. For a long time, there was no good way to get them into the game. We certainly did not want to give them administrative rights as a way to get them into the game. We certainly did not want to give them administrative rights to go and change the security on files and files shares, did we? Certification, also called attestation, has emerged as the security governance standard to draw the end user into the game. We are going to take everything we have learned through our analysis of all unstructured data, which we did to find the open shares, and the analysis of the data content and ownership, which we did to find where the sensitive data lives, and use it to ask the organization who ought to have access to what. We will start the process with the sensitive data so we know that that is properly locked down.

However, eventually we will run through the majority of our data. Maybe we will skip things like that open share HR uses, because we already know the answer. With this process running, we know that we are now making sure that the rules of the game are being minded by the people really playing that game. Security and IT can just be the referees – as it should be.

WHAT TO DO AFTER DAG FIXES EVERYTHING

Of course, Data Access Governance will not fix everything. It is always going to be part of that healthy breakfast of data security. However, there certainly are organizations using it to keep things well under control. Without controls to prevent more open shares from popping up, they just keep scans running on a regular basis so they can play the classic security game of whack a mole. As new open shares pop up, they get discovered and handled. You can do similar things for sensitive data propagating on the network, and also keep running certifications to make sure the access stays in line with business expectations. If the worst thing that happens is that you supply a secure environment through reactive, risk adjusted control like these, I am betting you will still sleep pretty well at night.

NEXT STEPS

Schedule a demo

stealthbits.com/demo

Download a free trial

stealthbits.com/free-trial

Contact us

info@stealthbits.com

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

stealthbits
NOW PART OF netwrix