netgovern™

MITIGATING INSIDER BREACHES: THE NETGOVERN PLAYBOOK

Unstructured data is often ignored because it's everywhere, and growing at an unbelievable rate. In other words, it's ignored because it's very difficult to manage. But, on average, unstructured data represents 80% of the information organizations hold. That makes unstructured data both an untapped source of opportunities and a major source of potential liability. As much as 1/3 of unstructured data is considered sensitive. Yet, organizations that do have security policies in place often fail to enforce them and access controls remain weak. In most cases, this is because protecting something unknown represents a serious challenge. Identifying sensitive content and governing data access should be priorities in any security strategy. But too often these issues are brushed aside and kept for later, because it is literally a mountain of work without the right tools.

DATA ACCESS GOVERNANCE – AN INCREASINGLY CHALLENGING GOAL

Unstructured data access is not easily governed. Staff changes, promotions, hiring, and firing and new & legacy systems are all moving pieces within organizations. Regulatory and threat landscapes are also constantly evolving, making security standards that were good yesterday, obsolete tomorrow. This makes it incredibly important and difficult for security staff to keep track of who has access to what and who should have access. Most of the time, security staff has no direct visibility into legacy systems and new permissions. They have no easy way of ensuring that end users have access only to what they need to do their current jobs. All of which increases the risk of insider breaches.

A FEW STATS FOR CONTEXT

In today's corporate data environment, file servers pose the second biggest risk of data breaches, right after databases. And as cleaning file and location permissions requires an immense amount of work without specialized tools, it's almost never done. As much as 24% of IT staff admit to never reviewing the list of end users who have access to data locations and file shares. And on the opposite side, only 24% say they would be able to detect end users accessing content they shouldn't. We can safely guess that the rest of the IT population has some visibility into access, but not as much as they need.

With 62% of end users admitting they have access to data that they shouldn't be able to see, stealing credentials and leaking sensitive information and intellectual property (IP) seems like it might be a promising career path.

Trick: Estimate the size of your unstructured and sensitive data

Size of your application database x4 = How much unstructured data you have

How much unstructured data you have /3 = How much of your unstructured data is sensitive

Source: https://resources.infosecinstitute.com/data-access-governance/#gref

THE ROT FACTOR

Most information security departments focus their time and money on detecting attacks and being ready for remediation. The "keep-everything-forever" approach to data and lack of visibility make their attack surface unnecessarily large while reducing the efficiency of the security measures they put in place. But why protect everything equally when data doesn't all have the same value? The truth is, 40% to 70% of the unstructured data organizations hold is redundant, obsolete, or trivial (ROT), and can be disposed of with no consequences. Only the remaining 30% of data is considered sensitive and needs to be protected. Seems like common sense, but organizations shouldn't spend money to store and defend information they don't need, and that puts them at risk.

THE DAG FACTOR

Don't underestimate Data Access Governance. It can't stop data leaks that inbound and outbound security should, but it can minimize the impact when those security measures fail. As an example:

John has worked in HR, and then in marketing. He still has access to all of HR's data, has access to the marketing file share, and the Finance one as he once needed access to some information to budget a marketing campaign. All he really needs to work is information related to marketing.

John willingly gives away his credentials by email to a malicious outsider pretending to be his company's IT manager. He just got phished.

With John's credentials, the scammer gains discreet access to a lot of data, and some that he wouldn't have if John's company had proper Data Access Governance: the list of employees with all their personally identifiable information including SSN & banking information, to budgets, M&A papers, and contracts, as well as future marketing campaigns and a list of prospect clients.

If John's company had a Data Access Governance program, the malicious outsider would still have gained access to marketing campaigns and prospect lists since the scam wasn't identified by inbound security technologies. But all other high-value data would have been safe.

Problems most often arise from these types of accounts

- Privilege creep
- Users with excessive privileges
- Stale accounts
- Orphan accounts

John is a victim of privilege creep because he gradually acquired privileges throughout the years, but no longer needs them. Users who have excessive privileges, meaning they inherit access rights and permissions that aren't justified are also a concern. Stale Accounts & Orphan Accounts pose another source of unnecessary risk, the former belonging to users who left the company, and the latter that don't seem to belong to anyone but still exist. These zombie accounts aren't in use but can still be compromised.

What are the types of threat that can be mitigated with DAG?

- Negligent insider
- Malicious insider
- Malicious outsider with the stolen credentials of an insider

A 2016 study concluded that in 50% of compromised accounts, negligent insiders were to blame, and in 13% of cases, malicious employees were the culprits. But outsiders, posing as insiders using stolen credentials, are also a significant cause of data breaches.

Who are insiders?

- Employees, current and former
- Contractors
- Third-parties
- Outsiders with insider credentials

Of course, the insiders who can do the most damage are those with privileged access to data. They will be targeted by social engineering attacks, but they are also the ablest to leak data themselves if they ever wanted to. The second group of insiders that you need to keep an eye on are contractors, and other third-party organizations with access to your data.

DAG FAILURE IN THE NEWS

There are more examples of data breaches caused by insiders or by outsiders with the right credentials in the news than you can count. But here are four that will help you get executive buy-in for your Data Access Governance program.

NEWS STORY 1

Data was leaked by a negligent employee

$93M class-action lawsuit filed against City of Calgary for privacy breach

The City of Calgary is being sued for $92.9 million, accused of breaching the privacy rights of more than 3,700 of its employees.

The class action lawsuit was filed Tuesday, alleging a privacy breach in June 2016. The court document claims a city staffer sent an email to an employee of another Alberta municipality, sharing the personal and confidential information of 3,716 municipal employees.

The personal information was contained in Workers' Compensation Board claim details and included medical records, Social Insurance Numbers, addresses, dates of birth, Alberta Health Care numbers and income details.

Read full article

NEWS STORY 2

Data was leaked by a contractor

What Businesses Can Learn About the Insider Threat From the NSA Contractor Data Breach

Former US National Security Agency (NSA) contractor, Harold T. Martin III, faces trial this June on charges that he stole an astonishing 50 terabytes of data

The huge haul contained documents far more sensitive than anything Edward Snowden made public. It is believed that his illegal activities began in 1996 and continued up to his arrest in 2016.

Read full article

NEWS STORY 3

Data was leaked by criminals with stolen credentials

Office 365 Phishing attacks create a sustained insider nightmare for IT

Since June, at least 30,000 Office 365 Phishing emails have fit the description of a sustained chain attack against Office 365 customers, but that number is based on just a few investigations, Fujitsu said.

The chained phishing campaign starts by sending emails in an attempt to collect usernames and passwords for Office 365 accounts. Once the victim compromises their credentials, the attackers then target that victim's address book - often filled with a mix of business and personal contacts.

The second stage of the attack attempts to leverage the first victim's existing relationships as an ice breaker, often using informal easy subject lines such as "FYI" in order to get the new victim to take an action.

The cycle is repeated as often as possible, with new victims keeping things going. After time, the harvested credentials are then used to compromise anything the victim has access to. Considering most organizations leverage Office 365 credentials for Exchange, One Drive, Skype, and SharePoint, and Office Store apps, the damage potential is serious.

Read full article

NEWS STORY 4

Data was leaked by a third-party

Verizon data of 6 million users leaked online

Verizon confirmed on Wednesday the personal data of 6 million customers has leaked online.

The security issue, uncovered by research from cybersecurity firm UpGuard, was caused by a misconfigured security setting on a cloud server due to "human error."

The error made customer phone numbers, names, and some PIN codes publicly available online. PIN codes are used to confirm the identity of people who call for customer service. […]

Chris Vickery, a researcher at UpGuard, discovered the Verizon data was exposed by NICE Systems, an Israel-based company Verizon was working with to facilitate customer service calls. The data was collected over the last six months.

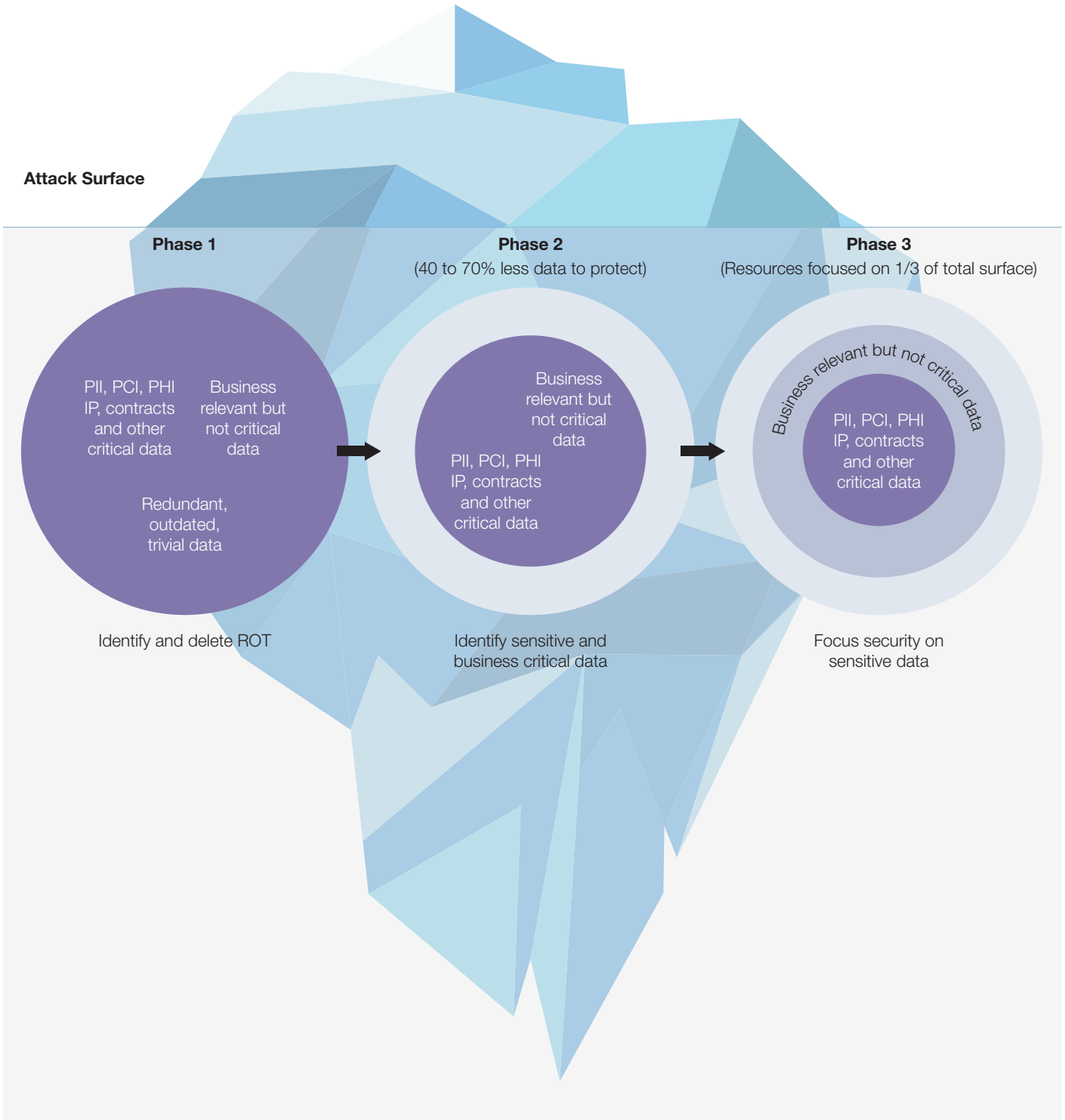
Read full article

In each of these cases, the consequences would have been dramatically reduced if an effective Data Access Governance program developed using best practices had been in place.

WHAT NEEDS TO BE DONE

Don't let your databerg sink your whole ship!

The first step to mitigating insider threat is to reduce your organization's attack surface. Redundant, Outdated, and Trivial (ROT) data needs to be identified and deleted. What should be left is business relevant, sensitive, and business critical data. Classifying it will help focus security resources on the risks.



Not everyone needs to access the same data and use it the same way

You can't control how employees access and use information or anyone who stole your employees' credentials for that matter. So who should have access to what? Ultimately, users should have the least amount of access rights and permissions to resources to efficiently do their job.

Access Rights

- Direct
- Indirect
- Inherited

To avoid complexities and inefficiencies, access rights should always be provided by assigning permissions at the highest level possible of your folder tree, which we call **inherited**. As organizations grow and change, creating new folder groups outside the tree structure and provide them with **indirect** access rights is also acceptable, even if it's not best practice. But the reality is that access rights are often provided **directly** to single users. It's a default method that requires less planning but creates confusion and security liabilities in the long-run.

Types of permissions

- Full Control
- Change
- Read

Just as not everyone needs access to the same data, not everyone needs the same type of permission. Ensuring end users have appropriate permissions to be productive can protect a lot of documents in case of Ransomware. If a user had access to some high-value files with a read but not write permission, they could work with the information they contain, and the ransomware would not be able to encrypt them.

THE STEPS

NetGovern's Suggested Process

1 - Identify sources of Redundant, Outdated, and Trivial data (ROT) and delete ROT to reduce the attack surface.

2 - Identify high-value files, sensitive data, and their locations.

3 - Report on who has access to those files and locations, and further investigate the access rights and permissions of end users with suspicious access to sensitive data locations.

4 - Report in hand, discuss with the owner of every data location where sensitive data has been identified, most likely business line managers, to establish if every user who can access their data has a valid need to do so.

5 - Remediate access rights and permissions that have been identified as non-necessary.

6 - Create or amend policies based on your findings.

7 - Monitor new accesses.

8 - Reassess policy and improve strategy.

The differentiator

It's easier to start the conversation with the data owners of all business units with a baseline of information to discuss. Be prepared with a report on who has access to their data and how, so access rights and permissions can be reviewed. Without a report, the approach would be to talk with data owners from many different backgrounds, and ask them who they think should have access to their data location. The first option is more reliable and facilitates collaboration. The second option makes the DAG problem so complex that it is often never tackled.

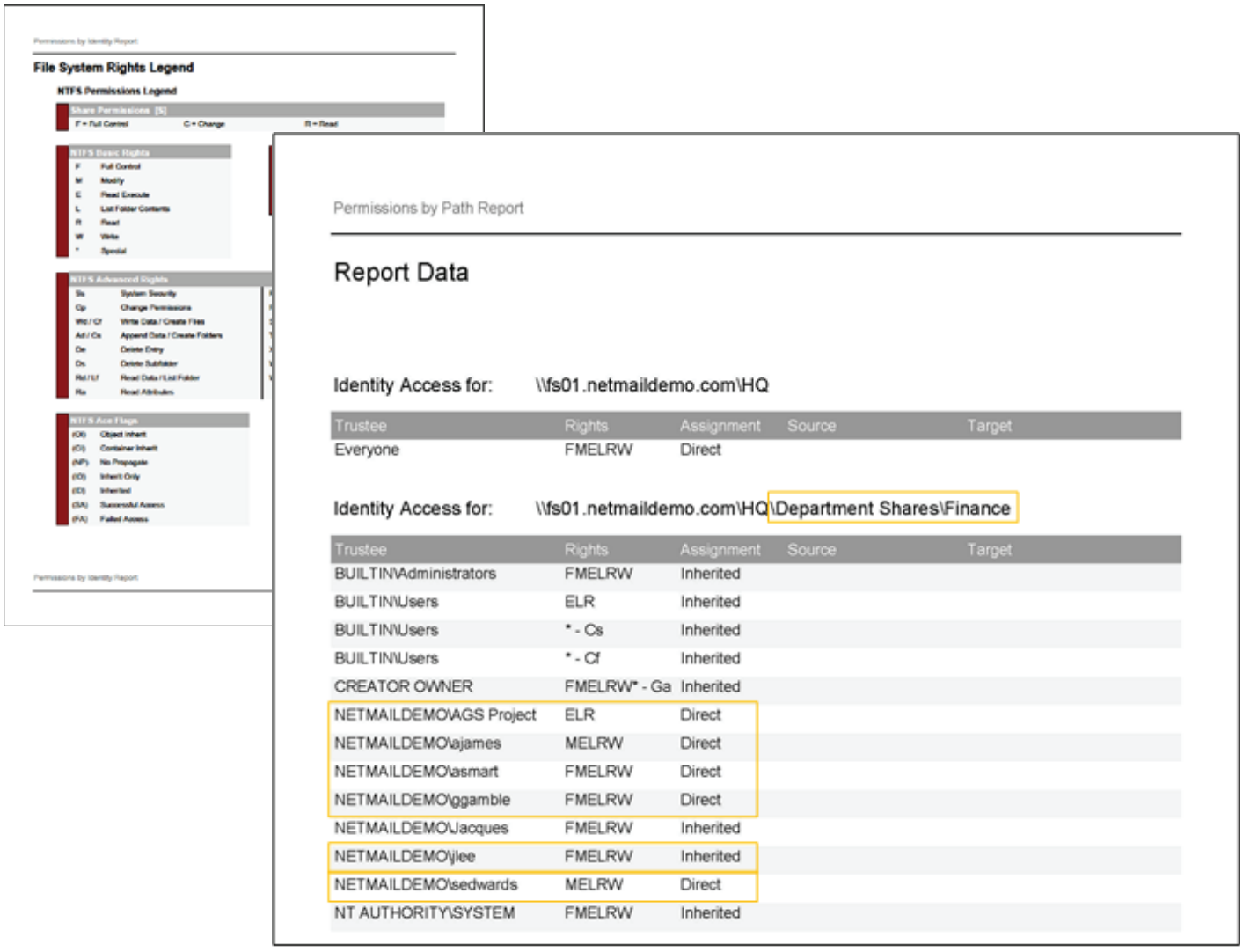
SCENARIO – NETGOVERN ANALYZE IS THE DAG ENABLER

NetGovern Analyze is a Data Access Governance enabler because it provides visibility on data accesses and permissions to facilitate remediation.

As an example, in the first report presented called **Permission by Path**, we'll examine Perchance Company's Finance Department Folder. We should find that most users who can access it work in the finance department, or are senior executives.

Findings that would be suspicious and require a deeper investigation:

- Former-employees who would still have access
- Employees outside of finance or do not have an executive role who have access
- Anyone with a Direct Access instead of an Inherited Access.



Permissions by Path Report

Report Data

Identity Access for: \\fs01.netmaildemo.com\HQ

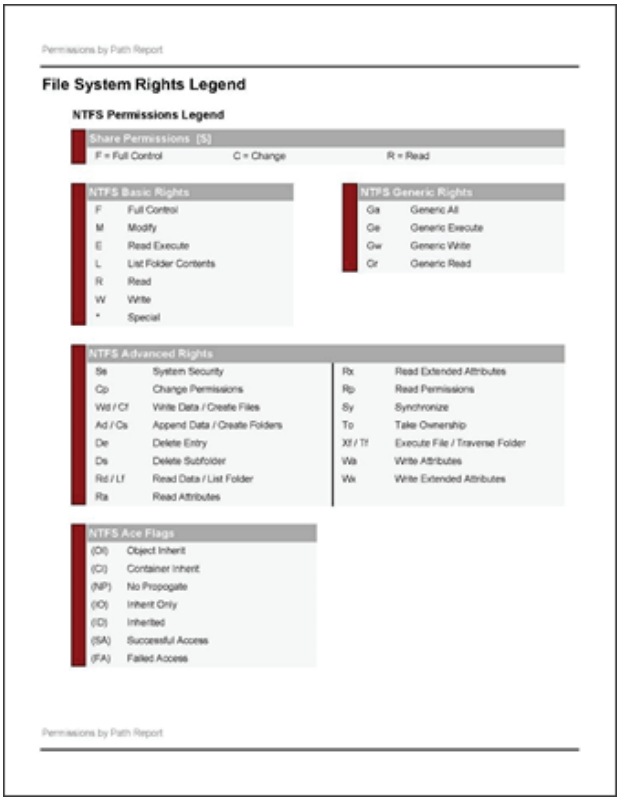
Trustee	Rights	Assignment	Source	Target
Everyone	FMELRW	Direct		

Identity Access for: \\fs01.netmaildemo.com\HQ\Department Shares\Finance

Trustee	Rights	Assignment	Source	Target
BUILTIN\Administrators	FMELRW	Inherited		
BUILTIN\Users	ELR	Inherited		
BUILTIN\Users	* - Cs	Inherited		
BUILTIN\Users	* - Cf	Inherited		
CREATOR OWNER	FMELRW* - Ga	Inherited		
NETMAILDEMO\AGS Project	ELR	Direct		
NETMAILDEMO\ajames	MELRW	Direct		
NETMAILDEMO\asmart	FMELRW	Direct		
NETMAILDEMO\ggamble	FMELRW	Direct		
NETMAILDEMO\Jacques	FMELRW	Inherited		
NETMAILDEMO\jlee	FMELRW	Inherited		
NETMAILDEMO\sedwards	MELRW	Direct		
NT AUTHORITY\SYSTEM	FMELRW	Inherited		

In the **Permissions by Path** Report, we have found that the user **jlee**, who does not work in the finance department or any of its child departments, has access rights to the finance file share. This is the first point to investigate with finance managers. We have also have found that the group **AGS Project**, as well as the users **ajames**, **asmart**, **ggamble**, and **sedwards** all had direct access, which should also be investigated.

In the next report, **Permissions by identity**, we can drill down into the access rights and permissions of the users identified as suspicious in the **Permissions by Path** report to ensure they don't have other unnecessary or suspicious access rights. For example, on page 108, we can see that the user **jlee** has access to business data from Perchance's Atlanta office, when he works at the Montreal HQ and does not collaborate with Atlanta staff, nor does he need access to their data for his work. A data breach from jlee's account would unnecessarily expose information from the Atlanta branch, when there's no need for him to access it in the first place.



Permissions by Path Report

File System Rights Legend

NTFS Permissions Legend

Share Permissions (S)		
F = Full Control	C = Change	R = Read

NTFS Basic Rights	
F	Full Control
M	Modify
E	Read Execute
L	List Folder Contents
R	Read
W	Write
*	Special

NTFS Generic Rights	
Ga	Generic All
Ge	Generic Execute
Gw	Generic Write
Gr	Generic Read

NTFS Advanced Rights			
Se	System Security	Rx	Read Extended Attributes
Cp	Change Permissions	Rp	Read Permissions
Wd / Cf	Write Data / Create Files	Sy	Synchronize
Ad / Cs	Append Data / Create Folders	To	Take Ownership
De	Delete Entry	Xf / Tf	Execute File / Traverse Folder
Ds	Delete Subfolder	Wa	Write Attributes
Rd / Lf	Read Data / List Folder	Wx	Write Extended Attributes
Ra	Read Attributes		

NTFS Ace Flags	
(OI)	Object Inherit
(CI)	Container Inherit
(NP)	No Propogate
(IO)	Inherit Only
(ID)	Inherited
(SA)	Successful Access
(FA)	Failed Access

Permissions by Path Report

*Click to see the **Permission by Identity** report sample and review **jlee**'s permissions at page 108.

RECAP

To ensure you are getting the most out of your digital security investment, mitigating insider threats is crucial. At a very high level, you can think of insider threat mitigation as a two-step process. First, you have to reduce the attack surface. Then you'll need to ensure all users have access to strictly what they need to do their work. To achieve this, you'll need the right tools, the collaboration of department heads or data owners, and some time.

About NetGovern

NetGovern's software enables regulated organizations to cost-effectively define and deploy vertical market ready Information Governance strategies in under 30 days, eliminating the "analysis-paralysis" phase that negatively impacts most enterprise data projects. Connect, Collect & Control petabytes of unstructured data stored in your file sharing, instant messaging, email and collaboration platforms, whether on-premise, on-cloud, or across hybrid systems. By providing comprehensive File Analysis (Audit), eDiscovery (Search), and Enforcement & Remediation capabilities, our clients can proactively organize, preserve, secure, and gain insight from what is arguably their most valuable asset – Information.

netgovern™

NetGovern, 180 Peel Street, Suite 333,
Montreal, QC, H3C 2G7
514-392-9220, info@netgovern.com