



INSIDER THREATS: Malice, Mistakes, and Mountain Lions

CONTENTS

OVERVIEW _____ 3

THE ANATOMY OF A BREACH _____ 4

OUR IRRATIONAL BIASES ABOUT RISK _____ 10

SIX TIPS FOR MITIGATING INSIDER THREATS _____ 12

ARE YOU WELL PROTECTED FROM INSIDER THREATS _____ 19

OVERVIEW

The goal of this whitepaper is to help you understand the most common insider threats and provide actionable tips to help protect against them. First we'll take a look at the actors involved in insider breaches and dissect the anatomy of a typical breach. Then we'll review some of the stats from [Verizon's annual DBIR \(Data Breach Investigations Report\)](#) and draw lessons from real world breaches. Next, we'll talk about irrational biases we have as humans and how they impact our ability to accurately quantify risk. Lastly, we'll walk through six things you should be doing to mitigate insider threats.

AN EPIPHANY IN ANGOLA

A quick and relevant story about the founding of Varonis in 2005. Our co-founders, Yaki Faitelson and Ohad Korkus, were working for NetApp on a project for a client in Angola, on the western coast of Africa. The client had commissioned hi-resolution digital photos of the ocean floor at great expense, and stored them on their NetApp filers. And one day, they were gone. Deleted.

The likely questions followed: Who did it? How did it happen? Who had access to them? Was it a competitor? Was it an accident? A hacker? An insider? ****Nobody knew.****

And so Varonis was born to give companies more visibility and protection for their high value information.

THE ANATOMY OF AN INSIDER BREACH

THE ACTORS



THE TURNCLOAK:

An insider who is maliciously stealing data. In most cases, it's an employee or contractor – someone who is supposed to be on the network and has legitimate credentials, but is abusing their access for fun or profit.

We've seen all sorts of motives that drive this type of behavior: some as sinister as selling secrets to foreign governments, others as simple as taking a few documents over to a competitor upon resignation.



THE PAWN:

This is just a normal employee – a do-gooder who makes a mistake that is exploited by a bad guy: whether it's a lost laptop or mistakenly emailing a sensitive document to the wrong person



THE IMPOSTER:

Whereas the Turncloak is a legitimate insider gone rogue, the Imposter is really an outsider who has acquired an insider's credentials. They're on your network posing as a legitimate employee. Their goal is to find the biggest treasure trove of information to which their "host" has access and exfiltrate it without being noticed.

THE SCRIPT



GET INSIDE: (IF NOT THERE ALREADY)

- Usually done by phishing or social engineering



SNOOP AROUND

```
PS C:\USERS\EDDARD>  
FINDSTR /R “^4[0-9]{12}  
(?:[0-9]{3})?$$”
```

- Enumerate current access; attempt to elevate
- Visa cards anyone?



EXFILTRATION

- Get the data out without sounding the alarm

It's best practice to assume that we have attackers on the inside already. Our goal is to: a.) minimize the damage any single account can do by reducing their access to need-to-know data, and b.) put in place sophisticated detective controls to alert administrators when sensitive data may be in jeopardy.

For Turncloaks and Pawns, there's no need to obtain credentials: they've been inside all along. However, Imposters will need to beg, borrow, or steal credentials to gain inside access. For this, phishing is definitely the way to go. Phishing and social engineering seem to be getting easier and easier. The 2014 Verizon DBIR claims that a phishing campaign of just 10 emails has a better than 90% chance of getting a click.^[1] It's like shooting fish in a...well, you know. You can see clearly why interior defense is increasingly important.

Next comes the discovery phase: snooping around to see where the juicy data lives and perhaps trying to elevate access. Does this require fancy spyware tools and scanners? Nope, plain old, slow Windows search with content enabled or the find and findstr commands will usually suffice, and will even work for mapped network drives.

Lastly, and perhaps the hardest part for the attacker, is exfiltration – getting the data out. This is where you're most likely to identify and hopefully stop the threat if you follow some of best practices we'll review later. Most insiders aren't master criminals, don't cover their tracks very well, and they'll likely assume the environment is unmonitored – which is sadly often the case.

[1] Moreover, the overall success rate of phishing emails is 18%!

BY THE NUMBERS

Figure 43. Top 10 threat action varieties within Miscellaneous Errors (n=558)

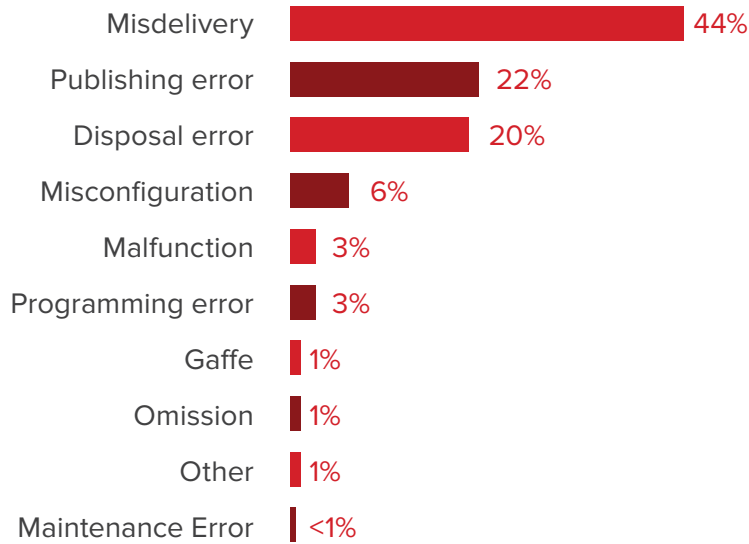
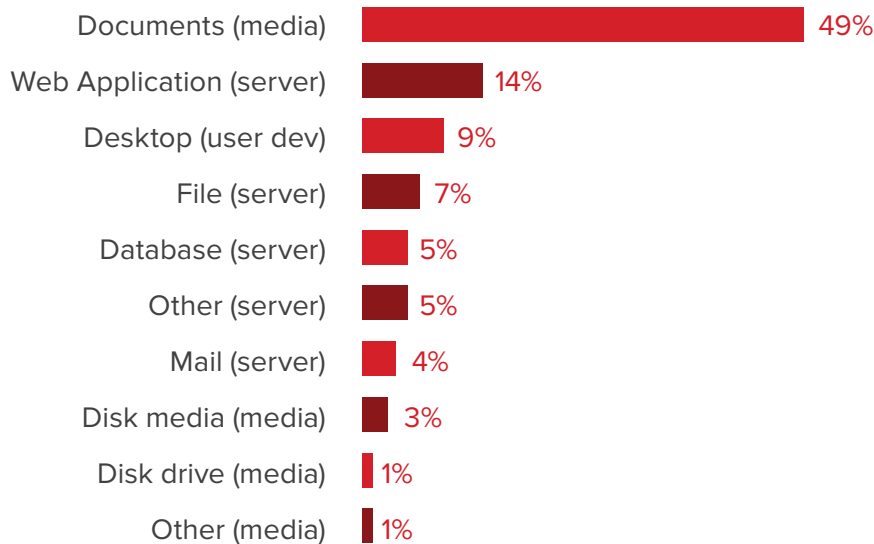


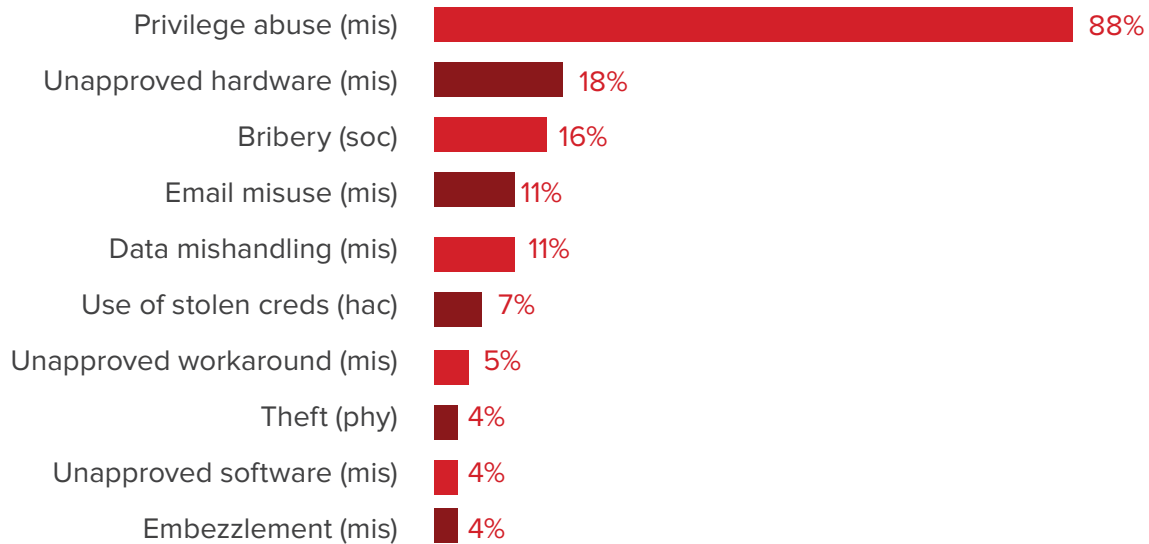
Figure 44. Top 10 assets affected within Miscellaneous Errors (n=546)



Insider threats are growing, and according to [CMU's study](#), the average incident results in \$800,000 USD of damage. Moreover, accidental exposures have become so common that the Verizon DBIR now has a separate category for them (separate from malicious).

In the 2014 DBIR, accidental exposures involving email, web publishing, etc. made up about 26% of all incidents. Within the insider threat category, mistakes account for about 60% of incidents and malice accounts for 40%.

Figure 30. Top 10 threat action varieties within Insider Misuse (n=153)



The above shows that among all insider threat actions, people are most often abusing the privileges they were granted by their employer. Most insider misuse occurs within the boundaries of trust. The problem is that, according to a recent study conducted by the [Ponemon Institute for Varonis](#), 71% of employees report that they have access to data they should not see, and more than half say that this access is frequent or very frequent. The surface area for privilege abuse is WAY bigger than it has any right to be.

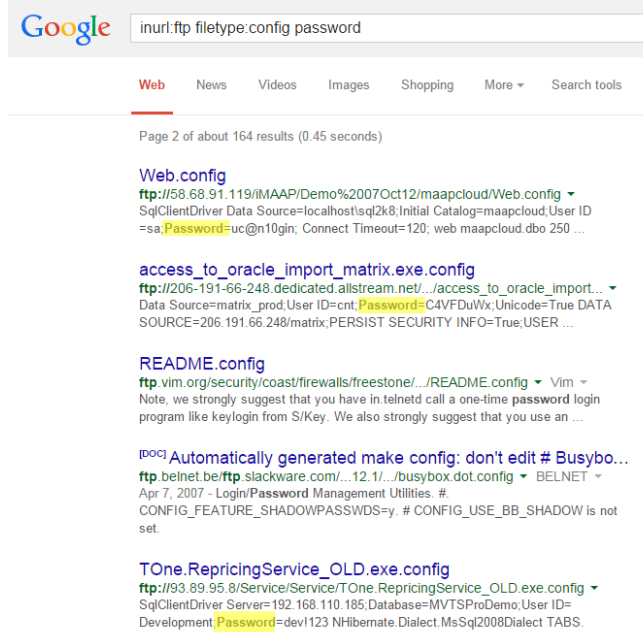
How do you stop someone when they're simply using the access you've given them? Hint: it's not easy.

Protecting against insiders is difficult for a variety of reasons. As humans, we naturally want to trust people, and we may feel guilty if we don't implicitly trust our colleagues. Additionally, we don't always know where our most sensitive assets are amongst the terabytes and petabytes of information that we store. Classification and risk prioritization is a needle in a haystack problem that simply cannot be solved manually.

Tracking insider behavior across multiple platforms can be complicated (e.g., email, files, SharePoint) especially when necessary IT resources aren't available.

OUR OWN WORST ENEMY

Sometimes, in life, we can be our own worst enemy. It's easy to see when you consider the images below. Credit to Troy Hunt for pointing these out in his fantastic talk: [Hack Yourself First](#).



These are real people tweeting photos of their brand new credit cards, numbers and all. Some are extremely excited, as you can see.

The above screenshot is a Google search. Did you know that Google indexes FTP as well as HTTP? Here you can see just how often people accidentally misconfigure their servers, allowing Google to index files like web.config that contain plain text passwords. Reputable companies that hire smart people aren't safe from errors like these.

The mistakes (to put it lightly) you'll find on Google and Twitter are often just as rampant inside the firewall, especially if you've got enterprise search that isn't well-tuned for security. If your access controls are broken and people have access to content that they shouldn't, deploying search makes it 1,000 times easier for employees – and hackers – to find otherwise well-hidden treasures.

Even without enterprise search, there are plenty of ways to snoop around using inconspicuous tools like the built-in Windows search or the find command mentioned earlier.

TARGET AS A TARGET

Target lost 40,000,000 records in 2014. They had lots of fancy tools watching the perimeter, but fell short when it came to securing insider access. We call this the candy bar syndrome: hard outside, soft inside. They got hit by an Imposter – a hacker who acquired credentials from a legitimate insider (a third party refrigeration vendor).

The Target case shows that you're only as strong as your weakest link, so if you give network access to a refrigeration company and their standard practice – which you can't control – is to put passwords on sticky notes next to the water cooler, you're toast. More commonly, credentials are easily phished through social engineering, acquired either through a password dump from a previous breach (I beg you: don't re-use passwords!), or flat-out guesswork.

It's vital to have a strategy for once the attacker is inside the building – to limit and review access and, as Gartner's Avivah Litan suggests ^[2]: use context-aware behavioral analytics to separate normal behavior from anomalous behavior (more on this in a bit).

It's extremely questionable as to why the refrigeration company had access to the POS systems in the first place. But even if you could explain that away as an honest mistake, shouldn't activity on such critical systems be watched like a hawk?

[2] <http://threatpost.com/avoiding-data-breaches-with-context-aware-behavioral-analytics/109679>

OUR IRRATIONAL BIASES ABOUT RISK

What do you fear more: being attacked by a mountain lion or slipping in the shower? What do you fear more: Heartbleed or a copy and paste mishap? It turns out that, as humans, we tend to greatly exaggerate risks that are sensational and beyond our control – like mountain lion attacks and nuclear radiation. Yet, we underestimate the mundane, but far more common risks that we can control like slipping in the shower or falling from a ladder.

Consider this the shower slip of a data breach: in February of 2014, Indiana University announced that 146,000 students' data, including social security numbers, had been exposed, not because of a hacker but because someone saved a file in the wrong public folder. They're not nearly as nefarious as the Stuxnet virus, but copy/pasters could be the single biggest threat to your business.

I know what you're thinking: "What are the odds that this type of breach will happen to me? 1 in 1,000?" Perhaps, but that's not nearly good enough.

Copy/pasters could be the
single biggest threat to
your business.

A STORY ABOUT TREES

Renowned scientist Jared Diamond spent 50 years doing field research in New Guinea. Early in his career, Mr. Diamond was on a trip when he proposed pitching his party's tents under a tall and beautiful tree in a forest. To his surprise, his New Guinea friends absolutely refused, explaining that the tree was dead and might fall on them and kill them. Diamond objected that the tree was solid and it would likely be standing for many years. The New Guineans were unconvinced, choosing instead to sleep in the open without a tent.

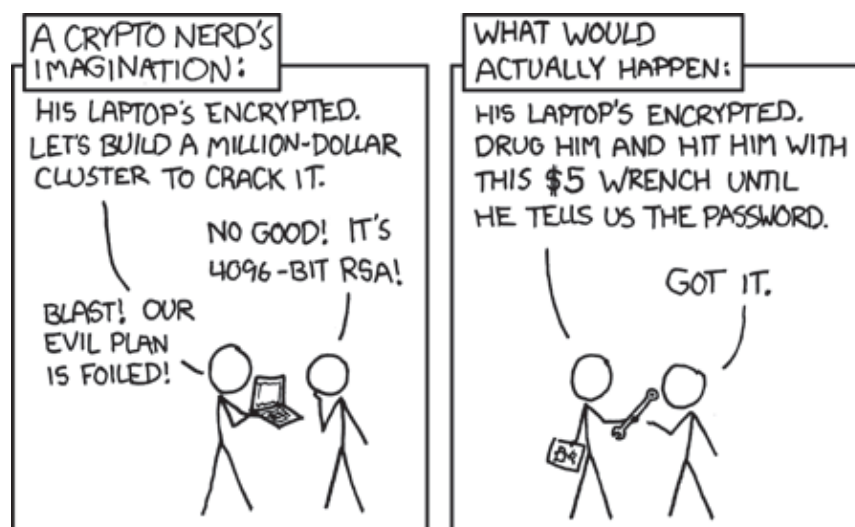
Diamond thought that their fears were unreasonable, verging on paranoia. In the following years, however, he came to realize that every night that he camped in a New Guinea forest, he heard a tree falling. And when he did a frequency/risk calculation, he understood the New Guinean's viewpoint.

If you live in a New Guinea forest and adopt the bad habit of sleeping under dead trees whose odds of falling on you that particular night are only one in 1,000, you'll be dead within a few years.

This simple calculation illustrates the greatest single lesson that Diamond learned from 50 years of field work on the island of New Guinea: the importance of being attentive to relatively improbable hazards that are encountered frequently. Over time, improbability pretty much becomes certainty.

FOCUS ON FREQUENCY

We've all met the engineer who will spend weeks obsessing over which password hashing algorithm to use, but fails to implement a solid password policy. If you find yourself being hyper-paranoid about dangerous but implausible attacks...stop! Do a quick risk/frequency gut-check to determine whether you're wasting time. You shouldn't be debating the strength of SHA-256 while your employees are emailing trade secrets to a Nigerian Prince.



Credit: <http://xkcd.com/538/>

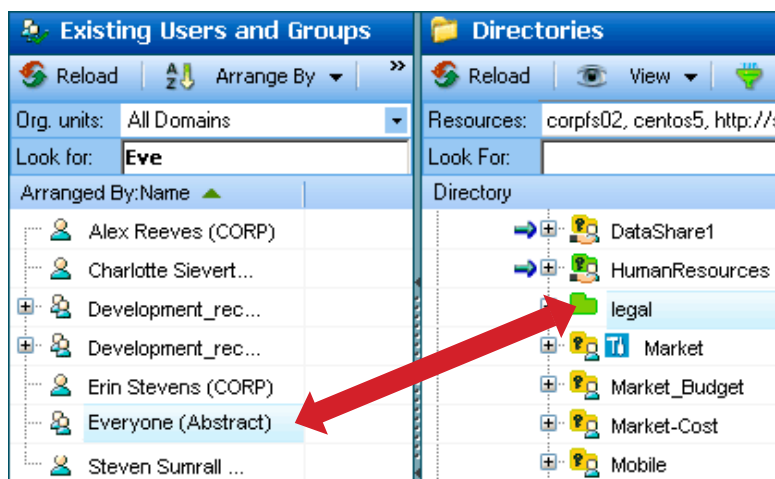
SIX TIPS FOR MITIGATING INSIDER THREATS

They're inside – we know that – so how do we minimize the damage that any one insider can do so we don't get Snowden'd? Here are six of the best tips for thwarting insider threats, based on nearly ten years of helping some of the biggest companies in the world manage and protect their valuable information.

TIP #1: ELIMINATE GLOBAL ACCESS

Many systems give you the option to grant global access to information via a special group like the “Everyone” group or “Authenticated Users” in Windows. When you grant access via a global access group, you're effectively saying, “I don't care what happens to this data.” I've seen global access applied to folders with millions of credit card numbers, socials, and more. It's a big blunt weapon that we should really stop using, save for information that is 100% public. When everyone can access data, it's very difficult to know who among the large set of potential users actually needs that access to do their job.

If we do know exactly who's touching the data, however, we can be surgical about reducing access without causing any headaches. Varonis DatAdvantage, for example, knows which folders, SharePoint sites, mailboxes and other repositories are globally accessible, and it also knows who has actually been accessing the data, so it can tell you exactly which people will be impacted if you were to remove global access.



In effect, DatAdvantage is doing an environment-wide simulation to answer the question, “What if I removed every global access group off every access control list (ACL) tomorrow. Who would be affected?” This capability is indispensable when doing global access remediation, lest you get a bunch of angry phone calls.

If you use global access groups, the single best bit of advice I can give you is to stop reading now and yank them. I’ll wait here.

TIP #2: ELIMINATE EXCESSIVE PERMISSIONS

According to a recent study we did in conjunction with the Ponemon Institute, 4 in 5 IT pros say their organizations don’t enforce a strict least-privilege (or need-to-know) data security model.

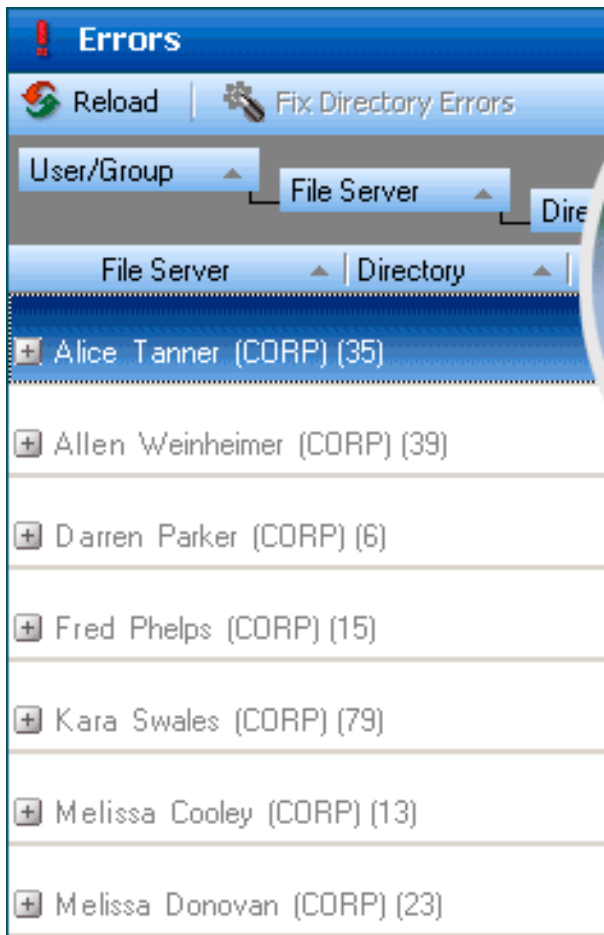
In most organizations, employees have way more access than they need, because:

- People change jobs, departments, responsibilities
- Temporary projects often require temporary access, but temporary access has a way of becoming permanent
- Consulting contracts start and end
- Permissions are granted accidentally
- People leave the company

Permissions creep plagues us all. It’s hard to prevent and can be even harder to remediate. Excessive access applies to both people AND software. If your web server has a vulnerability and it’s running under a privileged domain user that has access to the filesystem or, worse yet, network shares, any vulnerability in that web server software is now YOUR problem. Consider your software an insider, and limit its access to need-to-know.

Leverage Machine Learning

How often does the help desk receive a call from a user complaining that they have too much access? Never. DatAdvantage's recommendations feature uses machine learning to ensure that IT and data owners are aware the moment permissions can be safely revoked. What's more, DatAdvantage can be configured to automatically execute revocations on your behalf. It's like having one of those fancy vacuums that cleans up after you automatically.



Alice Tanner will lose access to data she has been using!







Auto-expire Temporary Access

I'd wager that I still have Domain Admin access at the company I consulted for in 1999. Temporary employees were granted access the same way as full-time employees and it's highly likely that the business people never told IT that my contract ended. With 5,000 employees, it's easy to lose track of these things.

For temporary employees, contractors, consultants, and project teams, entitlements should always be assigned an expiration date ****at the time they are granted****. This is your best shot at eliminating permissions creep. Access requests made via Varonis DataPrivilege can include an auto-expiration date and when that date arrives the software does the revocation for you in the background.

Periodically Review Entitlements

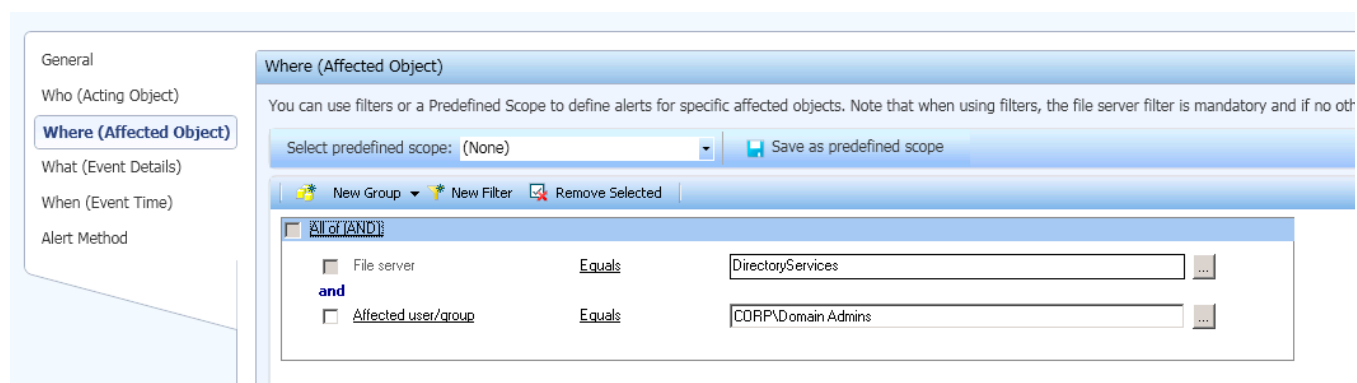
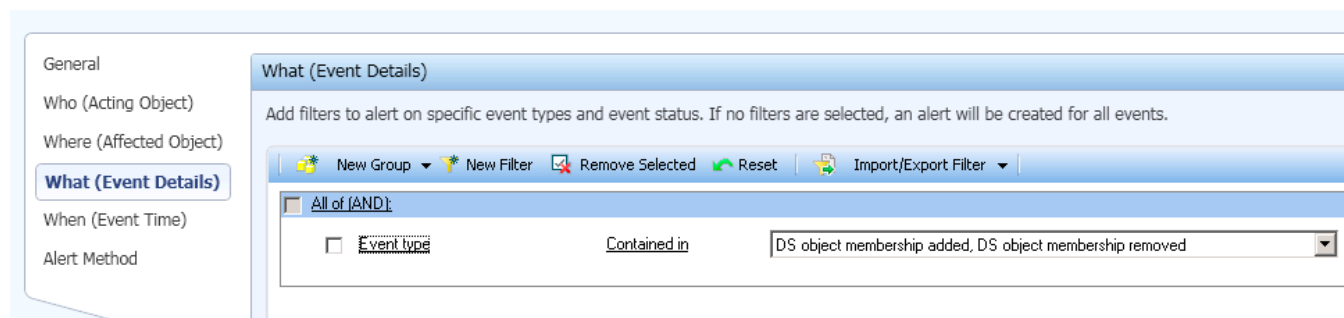
Even with machine learning and auto-expiry at your disposal, it still pays to have business users do periodic reviews. After all, they know the people who use the data. IT admins might not. Put the decisions in the hands of the people with the most context, and give them the power to make changes.

<input checked="" type="checkbox"/> Review only actionable objects			
<input type="checkbox"/> Review only entities that were not added by an automatic rule ?			
Status	Users	Permission	Decision And Explanation
	 Allison Schafer (CORP)	Exe-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	 Andrew Carlisle (CORP)	Exe-Write	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	 Andrew Weirich (CORP)	NA	<input type="radio"/> Keep <input checked="" type="radio"/> Remove
	 Andy Welch (CORP)	Execute	<input checked="" type="radio"/> Keep <input type="radio"/> Remove
	 Anne Lampkin (CORP)	Execute	<input checked="" type="radio"/> Keep <input type="radio"/> Remove

TIP #3: ALERT ON PRIVILEGE ESCALATIONS

Not only should you frequently perform an entitlement review on the Domain Admin group to ensure its members are legit, it is extremely helpful to setup alerts for additions to that group. Additions to privileged groups should be extremely rare, so it's nice to get an email alert or SMS message anytime that happens – especially if it happens outside of a change window.

I'm going to talk a lot about file analysis and auditing in a minute, but you'll also want to audit your Active Directory. It's the heart and soul of access control for many companies. If someone gets access to critical information via an Active Directory group, you want to know who did it, when, and why. Then use your file analysis logs to figure out exactly what the user did with their newfound access.



TIP #4: ALERT ON BEHAVIORAL DEVIATIONS

Remember that bit about the Target breach being prevented by context-aware behavioral analytics? It bears repeating. According to Avivah Litan of Gartner, the Target breach *and* the Snowden disclosures could have been prevented by behavioral analytics. Who are we to argue with Ms. Litan? She's super smart.

It's not enough to look at one thing, the way traditional IPS systems do. You have to look at events in context (e.g., Joe deleted 250 legal contracts five minutes ago and he works in the coffee shop. Hmmm.) Creating profiles of normal behavior on a per-user basis helps build context. If you baseline each user's normal activity, you can then alert when that activity spikes or they start behaving uncharacteristically.

You can do this if and only if you have file analysis software in place to record and analyze every event across your file sharing (and email) infrastructure. It's vitally important.

With file analysis you can do all sorts of cool things like:

- Detect when a sensitive file is created in a public folder and auto-quarantine it.
- Set up threshold alerts to sound when say, thousands of file copy events are firing within a minute. This will usually indicate that a user is doing a massive copy/paste from a network share to a potentially unmonitored endpoint: exfiltration.
- Monitor for normal business users creating or running EXE files on a server.

It's also a best practice to monitor for excessive activity outside of normal operating hours and to information beyond a person's normal departmental data stores.

Decrypting CryptoLocker

With file analysis software in your environment, you can start building profiles for strains of malware or common attack symptoms. Here is one we've used to very successfully combat CryptoLocker:

To boil it down for you: all file access activity is monitored (as it should be!) and threshold alerts are in place to detect rapid file modifications from a single user. When that happens, an alert is triggered which pings IT, checks the user's machine for the presence of CryptoLocker registry values, and then automatically disables the user. And because you have the audit trail, you can see precisely which files were encrypted and then use something like decryptcryptolocker.com to restore them.

1. Alert on more than 100 file modify events from a single user in under a minute

2. Alert triggers an action to:

2.1 Notify IT admins

2.2 Grab the username and machine

2.3 Check the machine's registry for key/value that CryptoLocker creates:
`Get-Item HKCU:\Software\CryptoLocker\Files).GetValueNames()`

2.4 If value exists, disable user automatically:
`Disable-ADAccount -Identity $actingObject`

TIP #5: SET UP HONEYPOTS

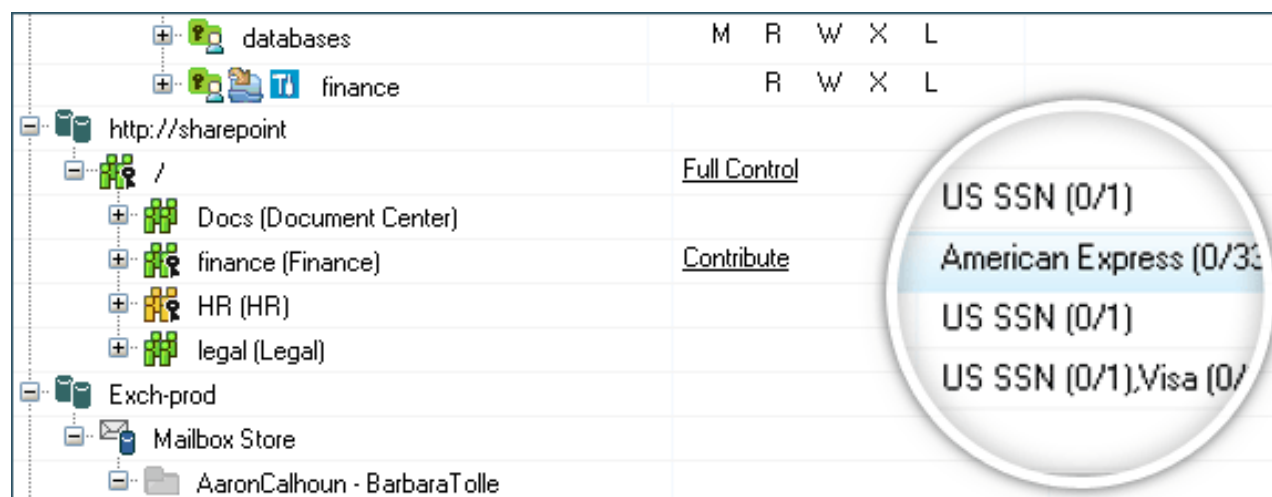
I always tell customers to create a honeypot – a shared folder with data that looks lucrative and is open to everyone and then watch and see what happens (hopefully via an automated file analysis application). This is a great way to find out who your Turncloaks might be and identify Imposters.

The recipe is quite simple. First, set up a shared folder that is open to everyone. Something like: X:\Share\Payroll or X:\Share\CEO. Then sit back and see who abuses it. You might find curious employees just snooping around or catch malware in action.

TIP #6: MONITOR HIGH-RISK PEOPLE AND DATA

It's very important to know where your crown jewels are, and that typically requires some sort of data classification technology. But it shouldn't end at discovery. Knowing that 700,000 files in your environment contain unencrypted credit card numbers is nice (though it may induce a panic attack), but it's not actionable. Your classification software should also answer questions like: Who owns the files (not the creator/owner attribute – who really owns them)? Who has access to them? What are they doing with it? Have they been opened? Copied? By whom? When? Once you add context through metadata, the classification results become much more actionable.

Once you find and prioritize the riskiest data sets, keep close tabs on the permissions, review access often (as I mentioned earlier), and set up some alerts to detect abuse and leakage. In addition to monitoring high-risk data, keep a very close watch on high-risk people, like IT administrators. It can be very difficult to monitor and police admin accounts because they usually need lots of access, but if domain admins are reading email in other people's inboxes and marking them unread, that's a red flag.



The image shows a screenshot of a file system tree with permissions and a data classification overlay. The tree structure is as follows:

Path	Permissions
databases	M R W X L
finance	R W X L
http://sharepoint	
/	Full Control
Docs (Document Center)	
finance (Finance)	Contribute
HR (HR)	
legal (Legal)	
Exch-prod	
Mailbox Store	
AaronCalhoun - BarbaraTolle	

A circular overlay on the right side of the screenshot displays the following data classification results:

- US SSN (0/1)
- American Express (0/3)
- US SSN (0/1)
- US SSN (0/1), Visa (0/1)

ARE YOU WELL-PROTECTED FROM INSIDER THREATS?

In two easy steps, we'll help you find risk areas, audit access, and understand where you're vulnerable to insider threats. It's free!

YES, I'D LIKE A FREE INSIDER THREAT ASSESSMENT!

ABOUT VARONIS

Varonis is the leading provider of software solutions for unstructured, human-generated enterprise data. Varonis provides an innovative software platform that allows enterprises to map, analyze, manage and migrate their unstructured data. Varonis specializes in human-generated data, a type of unstructured data that includes an enterprise's spreadsheets, word processing documents, presentations, audio files, video files, emails, text messages and any other data created by employees. This data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property and numerous other forms of vital information. IT and business personnel deploy Varonis software for a variety of use cases, including data governance, data security, archiving, file synchronization, enhanced mobile data accessibility and information collaboration.