IMPERVA®

# Top 10 Indicators of Data Abuse

PLAYBOOK

# Top 10 Indicators of Data Abuse

## Introduction

The threat from insiders is not a new phenomenon, but high-profile incidents have elevated enterprise focus on effective detection and mitigation of insider threats. Detecting insider threats, however, is challenging for organizations due to the combination of increased personal digital activities and more exposure and access to enterprise data then ever before. Since internal users have legitimate access to valuable information, it's difficult for organizations to discern between appropriate data access and a true insider threat incident.

Enterprises must trust their employees. That trust is critical to each step of the value chain, from day-to-day operations to pie-in-the-sky innovation, not to mention company culture. It's important, however, to also verify that the trust is well-placed. This involves monitoring access to sensitive and valuable data, and putting systems and guard rails in place that protect both your employees and your data. Most companies have some form of this in place - but even then - there are a lot of security alerts to sort through and many times it's tough to know what to look for when it comes to suspicious data access.

Despite our best efforts at education, prevention, and protection, breaches continue to occur for three main reasons:

- Organizations do not have the safeguards in place to identify risks and threats that involve insiders.
- Current solutions fail because they are designed to detect malware and tools that hackers use. They are absolutely not focused on the target of the attack: your data.
- You cannot isolate just the compromised insider or the malicious insider or just the careless insider - you need a solution for the whole problem.

*"The top three locations by volume where sensitive enterprise data is at risk: databases (49%), file servers (39%), and the rapid growth area for cloud service environments (36%)."*

2015 VORMETRIC INSIDER THREAT REPORT

## Insider Threat 101

By far the best definition of insider threat is from CERT[1] – "An insider threat is generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems." However, the insider threat does not consist of just malicious users, it also includes careless and compromised users. It is critical to understand the different types of insiders: compromised, careless, and malicious.

### Compromised Insiders

Insider users become compromised when a user's endpoint has been infected – often by means of phishing email and malware – and is being used by external actors to perform malicious activities without the knowledge of the user. Compromised credentials are another threat. Once compromised, the threat moves directly from the outside to the inside of the organization. This category includes compromised user accounts, as well.

### Careless Insiders

With so much sensitive content stored in Office 365 these days, it's imperative to have a way to identify sensitive or regulated data stored in services like OneDrive and to be able to take the appropriate measures to remediate risk.  A solution should be able to inspect content in real-time (by keywords, phrases, regular expressions, etc.) to ensure that sensitive corporate data is not maliciously or inadvertently leaked out of the organization and should be able to scan stored files for regulatory violations (e.g., PCI DSS, PHI, PII, HIPAA).  Similarly, if your organization is standardized on OneDrive, identifying files and data stored in unapproved file-sharing services is also critical for compliance and security purposes.

### Malicious Insiders

Edward Snowden is the best known malicious insider. Malicious users are the ones that deliberately steal classified, confidential, or sensitive data with the intent to cause damage. Incidents of this nature are typically motivated by convenience and financial gain[2]. This category of users receive the most attention, but compromised or careless users can also result in massive losses.

Insiders know where the data is stored, the value of the data, how to access the data and are largely unmonitored. In many cases, suspicious insider activity goes unnoticed given the lack of a data-centric approach to security and over-reliance on perimeter security

[1] National Cybersecurity and Communications Integration Center. Combating the Insider Threat. 2 May 2014.

## Protect Your Data from Inside Attacks

Accurately identifying potential data breaches requires deep contextual understanding of not just user activity, but the data users' access and how they access it. Without visibility into the data aspect, and an understanding of the true warning signs of abusive or inappropriate data access, one half of the equation is missing. The table below shows examples of common data abuse indicators, and the user and data details needed to do identify them. In this playbook, we examine the top 10 indicators of data abuse based on real world scenarios collected from live production data in several enterprise environments.

## Indicators of Data Abuse

| | SUSPICIOUS APPLICATION DATA ACCESS | EXCESSIVE DATABASE RECORD ACCESS | SERVICE ACCOUNT ABUSE | SLOW RATE FILE ACCESS | EXCESSIVE FILE ACCESS |
|---|---|---|---|---|---|
| USER | • User identity<br>• Client IP<br>• Server IP<br>• Client app | • User identity<br>• User department | • User identity<br>• Client IP<br>• Server IP<br>• Client app | • User identity<br>• User department | • User identity<br>• User department |
| DATA | • Database name<br>• Table name<br>• Data sensitivity<br>• Schema<br>• SQL operation<br>• SQL operation Type | • Database name<br>• Data sensitivity<br>• Table name<br>• Schema<br>• Number of rows<br>• SQL operation | • Database name<br>• Table name<br>• SQL operation<br>• SQL operation type | • File operation<br>• File path<br>• File name<br>• Folder type<br>• File share name<br>• Operation response time | • File operation<br>• File path<br>• File name<br>• File type<br>• File share name |

*"The thief who is harder to detect and who could cause the most damage is the insider the employee with legitimate access"*

U.S. DEPARTMENT OF JUSTICE. FEDERAL BUREAU OF INVESTIGATION. THE INSIDER THREAT. [2]

[2] The Insider Threat. https://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat

## 1. Database Service Account Abuse

### Description

An interactive (non-application) user logs into a database using a service account.

### Probable Threat

Compromised insider; Malicious insider; Careless insider

### Implications

An incident of this nature may indicate that user credentials have been compromised. Additionally, connection to a database service account by an interactive user bypasses the application's permission model and puts sensitive data at risk, as the service account is typically highly privileged. This activity masks the user identity from the database audit trail, making it impossible to uphold personal accountability.

### Case Study

Gathering data from a number of organizations, we uncovered that database administrators (DBAs) routinely use service accounts to access databases. This is often a security bad practice, but can also indicate that an internal user is attempting to operate under the radar. In one finding, a service account was used to access payment card tables that had never before been accessed outside of the designated application. This sensitive data access was characteristic of a human user, however, the use of service accounts to access information rather than using personal database accounts puts enterprise data at risk.

## 2. Excessive Data Access

### Description

A user accesses an unusually high number of database records or files, as compared to their typical behavior and the actions of their peer group.

### Probable Threat

Malicious insider; Careless insider; Compromised insider

### Implications

Incidents of this nature may be an indication of data theft. This behavior is the result of an unsanctioned export or modification of a large amount of corporate data from a database, or files have been copied off network shares. Once enterprise data moves outside the purview of IT control, the risk of data exfiltration greatly increases.

### Case Study

At an organization in the technology industry, we noticed an employee from the Technical Writing department in an organization copied many sub-directories of the file share—all located in a shared directory that belonged to the Technical Writing department. Altogether, the individual copied more than 100K files from the organization file share to their local computer over a period of three weeks. The employee performed some of these copies in the middle of the night and sometimes on weekends. Before this period, the user never copied this amount of files, and no one from her department or the rest of the organization copied this volume of files from the file share.

It is important to emphasize that the employee had permission to access all the files she copied. However, she copied very large volume of files from the file share, she was copying at abnormal times, and neither she nor her peers copy these amount of files on regular basis. The anomalous data access pattern triggered an investigation.

## 3. Suspicious Application Data Access

### Description

An interactive (non-application) user directly accesses sensitive application table data on a database.

### Probable Threat

Malicious insider; Careless insider; Compromised insider

### Implications

Individuals that directly access sensitive application data violate access privileges and expose the organization to the risk of a data breach.

### Case Study

Database systems typically work by granting unlimited data access privileges to database administrators (DBAs). Security best practices recommend that DBAs should have limited access to the data in the database. However, there is no real mechanism for enforcing it. In one customer environment, we noticed a DBA from the Information Technology department retrieved and modified multiple records from several internal PeopleSoft application tables on a specific day. These actions are alarming from several aspects. The first aspect is that the DBA did not access these tables through the PeopleSoft interface (he used the MS SQL Studio interactive query tool), and thus bypassed PeopleSoft logging and retrieval limitations. A second aspect is that the DBA retrieved an exceptionally high number of records from these tables and modified several thousand records in one of these tables. The third aspect is that he used a highly privileged designated PeopleSoft DB account to perform the table modifications.

When checking what information was accessed by the DBA, we noticed that these tables contained sensitive financial information that should never have been exposed to an employee from the Information Technology department, and certainly should not be manipulated outside of application processes.

## 4. Excessive Failed Logins

### Description

A user fails to log in to multiple databases a number of times.

### Probable Threat

Compromised insider; Malicious Insider

### Implications

An incident of this nature may indicate that a user is attempting to log in to one or more databases to which they were not granted access. Multiple failed logins may also imply that the user endpoint may be compromised and an attacker is attempting to gain access to the database.

### Case Study

Failed login attempts are a regular phenomenon in database access. Users fail to login to a database due to forgotten or mistyped credentials or due to password change. However, when a user fails to login to a database several times without success and never tries again, or when a user tries to access several databases in the organization without success, it is suspicious and may indicate that the user is not authorized to access the application.

In one customer environment, we noticed a member of an Information Technology department trying to login to an application that enabled access to sensitive financial information. After exploring the data, we identified that the employee failed to login to the application three times and then stopped trying. We continued our investigation and learned that the application that the user tried to access was a desktop application with preconfigured credentials using a designated database account. As such, the user was never supposed to fail in the login stage. In fact, none of the other users of the same application ever failed to login. Moreover, none of the other users of this application belonged to the Information Technology department.

When informing the security manager of that organization about the incident, we discovered that Information Technology members were not authorized to access this application.

## 5. Slow Rate File Access

### Description

A user accesses or copies an abnormally high number of files from the network file share (either their personal folder or department folder) over the course of one day.

### Probable Threat

Compromised insider; Malicious insider

### Implications

This incident may indicate that files were exported to an external network using a VPN connection, or to an external device (such as a USB drive).

### Case Study

A user copies around 2,000 documents from a department file share very slowly over the course of six hours. All files were copied automatically (by a single copy action) from a sub-directory in the file share. Each file copy took almost 14 seconds on average, while the average file copy takes less than 1 second in that organization. Although copying a large number of files is not uncommon, exfiltration of a high volume of files to an unidentified external machine is concerning. The fact that the copy took a very long time may indicate that the employee connected to the organization remotely, through VPN, and that they copied the files to a device outside the organization.

## 6. Machine Takeover

### Description

A user logs in to another user's corporate device to access a database.

### Probable Threat

Compromised insider; Malicious insider; Careless insider

### Implications

An incident of this nature may indicate that a corporate device has been compromised or has been maliciously taken over by an internal actor. In addition, sharing corporate devices violates security best practices.

### Case Study

Working with a customer in the media broadcasting industry, we uncovered a malicious help desk admin that accessed the laptop of a database administrator (DBA) using his domain admin credentials. Once he accessed the DBA's laptop, the Help Desk admin then used a SQL client set up with a service account to access the database. This unauthorized access was also flagged because the database access occurred outside of standard working hours, and the DBA attempted to access database tables containing Personally Identifiable Information (PII) which had never before been accessed by an interactive user.

## 7. Critical Credential Compromise

### Description

A machine that has been compromised attempts to access sensitive data resources.

### Probable Threat

Compromised insider

### Implications

When a hacker takes control over a user's machine they can automatically access any resources to which the victim has access, putting sensitive data at risk.

### Case Study

One of the most obvious cases of an advanced attack, is the usage of stolen credentials. It is rare to catch a glaring red flag of a compromise, statistically speaking. However, this was exactly the case in one incident. This time, planted credentials inside Windows Vault and Internet Explorer, were dumped and used by an attacker. This type of behavior is not only indicative of a compromise, but usually of a manual operator that has a backdoor into the organization. While the attacker had no idea his activity was already detected, we were able to determine the source and scope of the attack, and completely remove the threat from the network.

## 8. Cloud Application Account Takeover

### Description

Compromised account via unauthorized account takeover

### Probable Threat

Compromised insider

### Implications

An unauthorized or malicious user may have access to all data, including sensitive or regulated data, within an account. In this case, enterprise data could be deleted, shared, modified, or manipulated.

### Case Study

Cloud accounts are more likely to be accessed from BYOD and shared endpoints making them more susceptible to compromise. During an engagement with a company in the retail industry, we found several instances where cloud accounts were compromised. In one such case an attacker got hold of a legitimate user's Microsoft Office 365 login credentials through spear phishing, a popular social engineering attack. Once the attacker had the credentials, they accessed the compromised user's Office 365 account and downloaded sensitive documents from the OneDrive account.

## 9. Unusual Cloud Access Attempts

### Description

Many unsuccessful logins within a short period.

### Probable Threat

Malicious insider; Compromised insider

### Implications

An incident of this nature may be indicative of a brute force attack where the bad actor is attempting to access a cloud app account to delete, exfiltrate, share, or edit data.

### Case Study

Credential stuffing typically targets cloud and SaaS applications. Usernames are often easy to guess as the default typically is the user's corporate email address. In one case, a user's Dropbox account was under attack with the many different passwords being attempted within a short period. Too many unsuccessful logins from the same IP address back to back or are indicators of a brute force attack. In this case the attacker was unsuccessful, but the failed logins would have gone unnoticed. If the attacker had succeeded, they would have been able to perform any number of actions on the data – edit, delete, share, or export.

## 10. Suspicious SaaS Data Export

### Description

A user downloads a high volume of data from a SaaS application.

### Probable Threat

Malicious insider; Compromised insider; Careless insider

### Implications

Incidents like this one could lead to data exfiltration, whether done maliciously or inadvertently. The final outcome could be the loss of sensitive or regulated data.

### Case Study

Data exports from the cloud/SaaS applications are harder to track given the many different SaaS applications in use by enterprises today. Most employers know that when an employee is about to quit, the employee tends to make personal copies of intellectual property or sensitive data. In one such case, we highlighted a sales representative downloading a large number of Salesforce reports onto his personal mobile device. On closer inspection, we found out that the sales representative had just received a bad review from his employer. The individual figured his days were numbered at his current job and decided to take confidential, proprietary information with him to his next employer.

## Conclusion

It is not a matter of "IF" in regards to insider threats, it is a matter of "WHEN". The examples mentioned here are just the tip of the iceberg. There are many approaches out there that promise ultimate protection against insiders, but what we have realized over many years of monitoring access data is that detection is key, and prevention can be effective only when false positives are eliminated and the number of alerts are manageable for the security team.

While it may appear humanly impossible to track all insider threats in an enterprise, the use of machine learning, deception tokens along with the context of data access can achieve the end goal of detecting anomalous behavior early enough.

## About Imperva CounterBreach

Imperva CounterBreach protects enterprise data stored in enterprise databases, file shares and SaaS applications from the theft and loss caused by compromised, careless or malicious users. By dynamically learning users' normal data access patterns and then identifying inappropriate or abusive access activity, CounterBreach proactively alerts IT teams to dangerous behavior. CounterBreach also uses deception technology to deterministically identify end-point devices that have been compromised by external attackers, adding additional context to user data access learning.

## About Imperva

Imperva® (NYSE: IMPV), is a leading provider of cyber security solutions that protect business critical data and applications. The company's SecureSphere™, CounterBreach™, Incapsula™ and Skyfence™ product lines enable organizations to discover assets and vulnerabilities, protect information wherever it lives - on-premises and in the cloud - and comply with regulations. The Imperva Application Defense Center, a research team comprised of some of the world's leading experts in data and application security, continually enhances Imperva products with up-to-the minute threat intelligence, and publish reports that provide insight and guidance on the latest threats and how to mitigate them. Imperva is headquartered in Redwood Shores, California