

Insider Threat Playbook:

How to Deter Data Theft by Departing Employees



Table of Contents

Introduction	3
Reasons Why Departing Employees Can Be a Security Nightmare	4
The Motives behind Data Theft by Departing Employees	6
Top 3 Ways Departing Employees Steal Your Data	7
How to Mitigate the Risk of Data Theft by Departing Employees	9
How to Spot Data Theft Attempts by Departing Employees with Netwrix Auditor	11
About Netwrix	14

Introduction

Picture your IT infrastructure as a castle where your highly critical data resides. Just a few years ago, to defend those “crown jewels,” you could simply build a moat around the perimeter of the castle. However, times have changed. Businesses still spend billions of dollars a year on firewalls and intrusion-detection systems to try to protect their data from hacking, but often the threat is already inside the castle: their own employees.

Consider data theft by employees who are about to leave the company. In today’s digital world, the problem of data theft by departing employees goes far beyond stealing the names of a few customers or a product design sketch. It can mean the loss of gigabytes of critical corporate intelligence and legally protected information like customer cardholder data. Plus, ex-employees have even more avenues for using the data they steal — they can use it against their former employers, leak it to competitors, sell it to the highest bidder or simply publish it on the internet.

Employees taking sensitive company information with them when they leave their jobs might seem like the stuff of nightmares, but it’s actually a common true horror story. [Biscom’s](#) research, for example, found that one in four respondents took data when leaving a company. It’s easy to find examples in the headlines; just look at the recent cases with Uber or Gucci.

Organizations are getting wise to this threat: According to Kaspersky’s IT Security Risks Survey 2017, 52% of businesses say that employees are their biggest weakness in IT security, with their careless actions putting business strategy at risk. If you’re not in this 52% yet, it’s high time to start treating departing employees as a real threat.

In this eBook, we’ll walk you through the most common reasons why departing employees can turn into a security nightmare, identify their motives, review the ways they can steal your data, and provide some tips you can use to mitigate the risk of employee data theft.

Reasons Why Departing Employees Can Be a Security Nightmare

Let's start by taking a look at the five top reasons explaining why employees can turn into the villains in your security horror story:

1. HR is from Venus and IT is from Mars

In many organizations, communication between HR and IT is so difficult and rare that they might as well be on two different planets. This disconnect creates a great environment for malicious employees who are about to depart. If the IT team is not notified promptly about terminations, malicious insiders have time to use their privileges to copy sensitive data they want to take along with them, or erase important data they don't want to leave behind. Of course, lack of communication isn't the only way departing employees retain access privileges after they leave. Sometimes, the IT team is so overburdened and understaffed that they fail to promptly deactivate accounts even though they know an employee has departed. Either way, the result is the same: a gaping security hole.

2. There's no Idiot's Guide to help employees know better

Failure to educate employees about what they are and are not allowed to do can easily lead to cybersecurity incidents. In fact, [Kaspersky's 2017 IT security risk survey](#) found that careless or uninformed employees are second only to malware when it comes to causing serious security breaches, playing a role in 46% of cybersecurity incidents. Given that HR departments often don't make it priority to educate staff about what is behavior is acceptable and what is illegal, it's no surprise that some departing employees are simply unaware they are doing a bad thing when they take documents or a list of contacts with them to another employer.

3. What to expect when you're inattentive

According to the Biscom report, 90% of respondents said their primary reason for stealing data when they left was that their employer did not have a policy or technology in place to prevent them from doing it. Even if they are not motivated primarily by malicious intent towards the employer, many people will consider taking confidential information with them that may be of use in their new role. The Biscom research found that 85% of employees who stole data took only things they had created, following the philosophy, "what was made by me belongs to me." In contrast, only 25% percent of respondents took data they had not created.

If there's no strict policy in place specifying the actions that have to be taken when an employee is about to depart, it's almost impossible for IT teams to even track what data has been copied or deleted until it's too late. The growing popularity of BYOD adds to the problem, especially if device management is poor. For example, when an employee's contract is terminated, the IT department rarely asks that employee to display their personal devices to ensure all the critical assets have been erased and can't be assessed later.

4. A series of unfortunate accounts

Too often, an employee who leaves still knows the passwords to team accounts for important systems or apps, such as Cloud Share or Dropbox. For personal reasons or upon the request of a new employer, the former employee can use those credentials to access and misuse your data. Changing the passwords to shared accounts frequently, and especially whenever an employee leaves, can greatly reduce the risk of unauthorized access to critical data, but few organizations make it a priority to faithfully follow this fairly simple best practice.

5. 50 shades of conspiracy

The scariest story is when employees from other companies, such as competitors, conspire with employees who are about to leave to steal trade secrets in order to advance their business. These cases can result in lengthy and expensive legal proceedings, and even put companies out of business.

The Motives behind Data Theft by Departing Employees

These days, almost all sensitive data is stored electronically, from confidential trade secrets to customer information to employee records and more. Employees need access to certain bits of that data to do their jobs. Unfortunately, some of them believe that if they work with particular data every day, it belongs to them, and they have a right to simply take it along when they leave the company. Others know they are stealing but do it anyway.

The motives for data theft can vary widely: setting up a competing business, selling the information on the black market, taking revenge on the former employer and more. But all corporate data theft cases can be divided into the following categories:

- **Data theft driven by a malicious intent.** Employees with a malicious intent often exhibit unusual behavior. For example, they might access files they haven't looked at before, copy a large number of files or forward important emails to their personal mailboxes. Admins with privileged rights might make critical changes without authorization or approval in order to gain more permissions. Any of these actions could be a sign of privilege abuse that could lead to data theft.
- **Data theft without a malicious intent.** Insiders can also take actions that put data at risk without malicious intent. For instance, users might copy files to their personal devices in order to use them for a project, without even realizing they are doing something illegal and dangerous. Even if the users would never misuse the data they copied, it can more easily be obtained by bad actors. Therefore, the IT team has to ensure these kinds of actions can't slip under their radar and jeopardize data security.
- **Data theft as a result of data misuse.** Classic examples of data misuse are accidentally attaching the wrong sensitive data to an email or sending the right sensitive data to the wrong recipients. Whether the misuse is the result of inattention, stress or ignorance of proper workflows, it can easily result in just as much damage as the other types of data theft.

Top 3 Ways Departing Employees Steal Your Data

Why do people take a risk and steal from their employers? According to the [2017 Verizon Data Breach Investigations Report \(DBIR\)](#), the primary motive is financial gain, which accounted for 60% of breaches in 2016. This is not a surprise. Personally identifiable information (PII) is extremely valuable on the black market, and stolen intellectual property (trade secrets, sales projections, marketing plans and so on) can be worth billions of dollars to competitors. Less frequent motives for data theft are cyber espionage for career development, revenge, whistleblowing and stealing data for fun — but, of course, these motives can also have a strong financial component.

So how exactly does data theft play out based on these different motivations? Here are three case studies that illustrate the process, and the consequences for the victim organizations.

Case #1. Data theft for financial gain and career development

[Rogue employee jeopardizes the future of Uber's self-driving car strategy \(2017\)](#)

Here's how quickly a dream can turn into a nightmare. Uber is one of the most successful and well-known companies in the world. To advance its goal of developing self-driving cars, it acquired a startup called Otto, which was developing a technology Uber needed, and hired its all-star team, including Otto's founder, Anthony Lewandowski. Uber seemed well on its way to dominance in the hot new area of autonomous vehicles.

A year later, Uber's lesser known competitor, Waymo (a part of Alphabet, which is also the parent company of Google), sued Uber for trade secret theft.

According to Waymo, Lewandowski stole some 14,000 confidential technical documents, blueprints, design files and other files as he was leaving Waymo and used that intellectual property to found his startup, which was later acquired by Uber. Now Uber is in a very tough position. It may face criminal prosecution not only for using stolen technology in the production of its self-driving vehicles, but also of actively covering up the trade secret theft.

The case is under investigation and the trial has been postponed to December 2017, but both companies are already involved in a series of intense public hearings. This certainly doesn't look good for Uber, especially considering the fact that the company is facing another federal investigation for allegedly violating the U.S. Computing Fraud and Abuse Act (CFAA).

It's too early to predict how the case will end, but stakes are already high: Companies are fighting for the right to develop a technology that may be as significant for the industry as the invention of the automobile itself.

Case #2. Deliberate data theft or damage

A plastic surgery drama in Beverly Hills (2017)

It would be horrifying to discover that photos and videos of your plastic surgery have been posted on the internet — especially if you're a celebrity whose face can be readily identified by millions of viewers. But that's exactly what happened to patients of famous Beverly Hills plastic surgeon Dr. Zain Kadri.

In 2016, Kadri hired an employee who worked first as a driver and translator, and then moved on to data entry and answering phone calls. She either quit or was fired in 2017 after being accused of embezzling from the company.

But apparently she misused her insider privileges in other ways. According to a statement from Kadri's practice, she also used her corporate smartphone to take pictures of patients' medical records and credit card information — and also took inappropriate photographs and videos of patients before and during surgery.

The case is still under investigation; however, Kadri believes that the primary motive here is revenge. At least some of the videos and photos were made public on Snapchat and Instagram — a strategy that could draw ire towards Dr. Kadri from his celebrity clientele and hurt his practice. So far, there is no evidence that the employee was financially motivated or hired by a competitor.

Case #3. Human mistakes or negligence

FDIC faces a series of data breaches due to employee mistakes (2016)

In February 2016, an employee at the U.S. Federal Deposit Insurance Corporation (FDIC) was leaving her job. On her last day at work, she downloaded her personal files from her work computer to a USB drive and took it home. Three days later, the FDIC's data protection software detected that 44,000 customer records, including PII, had been accidentally taken along with her personal data. The FDIC promptly contacted the ex-employee and asked her to return the device and sign an affidavit stating she did not use or share the information.

This case wouldn't be so worrisome if the FDIC hadn't already experienced at least five similar security incidents, with departing employees accidentally transferring company data to personal storage devices — including highly sensitive data like loan and banking information. Unlike the February 2016 incident, not all the earlier breaches were immediately handled and reported by FDIC, which led to a series of hearings and fines from regulatory bodies.

Although the FDIC seems to have taken to heart the need to report security incidents promptly, the management team should really ask two key questions: First, how long will it be before the organization finally updates its security policies and makes sure that employees follow basic cybersecurity rules? And second, were all of these breaches truly unintentional?

All the cases above have one thing in common: It took less time for ex-employees to obtain sensitive data than for organizations to detect and investigate the incident. Indeed, stealing an employer's data doesn't take long, but detecting a malicious insider in your company's network can take months or years.

How to Mitigate the Risk of Data Theft by Departing Employees

Right about now, you might be ready to jump into buying one or more of the various threat detection tools on the market. But before you do that, it's important to get a better understanding of exactly what needs your attention. Here are some tips and best practices:

- Consider Gartner's CARTA approach. By understanding the changing risk landscape and placing only the trust appropriate at a given time in your employees, you can limit the damage any user can do.
- Recognize that there's no single breakthrough pill that can beat all threats to your data. You need a set of reliable solutions, each with specific functionality.
- Know what data you need to protect. Discover and inventory your sensitive information and where it resides, so you can identify patterns in user activity related to that data storage and spot anomalous actions that could be threats.
- Establish data security governance policies for the entire organization. Be sure that they focus on identifying and mitigating the risks to data security, but also are aligned with business needs.

Once you have a picture of what has to be in place, you need the right technologies to bring your strategy to life. As a starting point, we've put together two sample toolkits — essential and advanced — that can help you perform routine monitoring and management tasks across your IT ecosystem, as well as detect and reduce potential threats (like employee data theft).

The essential toolkit includes a few basic technologies that are handy in mitigating the risk of employee data theft:

- Basic rules and policies are your first line of defense. For example, consider isolating emails sent to personal email accounts, prohibiting storage devices such as USB thumb drives, enforcing the least-privilege principle, and monitoring all changes to privileged group membership.
- A process for revoking privileges upon user termination according to best practices (provided it is diligently followed across your organization, of course) will help you ensure that no departing employees retain any access to your IT infrastructure when they are no longer in the game.
- Auditing tools with log collection and reporting functionalities are must-have for staying on top user activity. For instance, they will help you identify who read what sensitive data, or how many times a specific user tried to access a shared mailbox and what exactly he or she did there. If you have a bigger budget, a SIEM solution will be your best bet here.
- Integrated data loss prevention (DLP) solutions will help you identify sensitive data and ensure it is not sent outside the organization without your notice by securing web and email gateways, encrypting emails, securing cloud access, and more.

The advanced toolkit is for experienced security pros that need more than what the technologies in the essential toolkit have to offer:

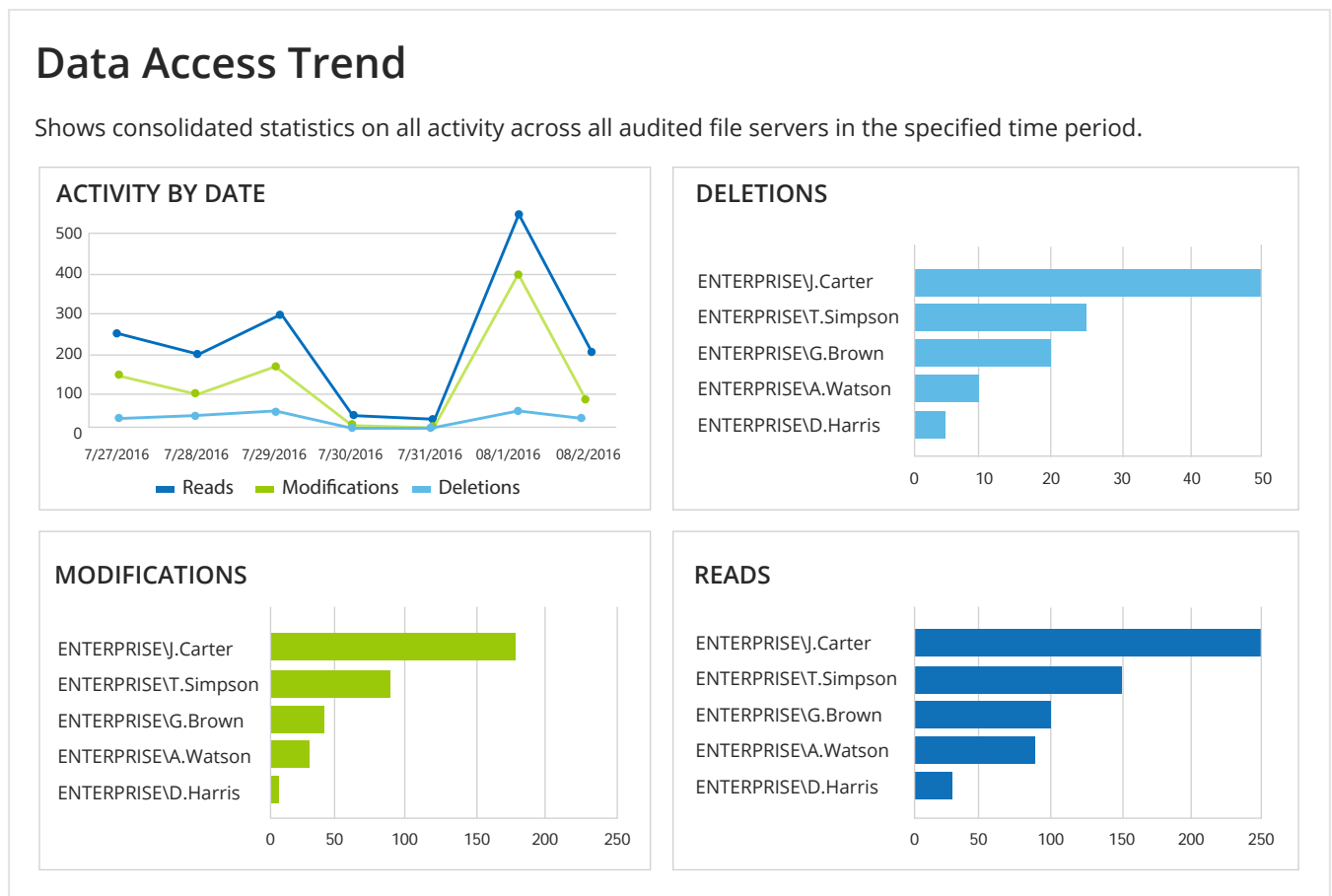
- Identity and access management (IAM) technologies enable you to improve information security, optimize workflows, reduce errors and streamline compliance — all while covering the majority of identity-related issues, including compromised accounts, identity theft and data theft.
- Privileged access management (PAM) helps you ensure that administrators and other privileged users have only the permissions they need at any given time to do their jobs, and to centrally monitor the activity of those users.
- Cloud access security brokers (CASB) improve data security in the cloud by delivering visibility into user activity and notifying admins about suspicious actions that could indicate data theft by insiders or an external attack.
- UEBA or SIEM solutions with user behavior analytics help you identify suspicious user activity in your on-premises environment, so you can take the necessary measures to reduce risk before data theft occurs. For hybrid environments, coupling a UEBA or SIEM with a CASB constitutes top-to-bottom visibility.
- Employee monitoring works like a surveillance camera, tracking all employee activities, including what data they read, which files they copy, whom they send emails with critical data to, who they talk to on the phone and more.
- Data classification and discovery solutions help you identify what data you have, determine which of it is highly sensitive and analyze how this data is used, so you can reduce risks such as insider data theft.
- Security services, such as penetration testing, can simulate an attacker exploiting vulnerabilities across your environment, and then guide you about how best to choke off the attack. If you don't have an advanced security team on staff, security services provided by third-party experts can be very valuable.
- Enterprise DLP solutions enable you to incorporate more sophisticated data protection techniques and minimize the risk of data loss at your endpoints with centralized management, support for advanced policy definition, and event management workflows and reporting.
- Data protection technologies that can vary from a particular capability in a single solution to a set of tools with blocking, encryption, tokenization and data masking functionality.

How to Spot Data Theft Attempts by Departing Employees with Netwrix Auditor

To secure your company's intellectual property, financial records, personally identifiable information and other valuable information from company data theft, Netwrix Auditor offers a set of predefined reports and overview dashboards that help you prevent business-critical data from walking out of the door with departing employees.

1. Monitor data access trends

Spot any spikes in data reads, modifications and deletion attempts so you can respond to suspicious activity in time to prevent a data breach.



2. Keep an eye on user activity outside business hours

Keep track of users who are unexpectedly working with data during non-business hours and collect evidence for security investigations.

Activity Outside Business Hours

Shows users who performed any actions outside their business hours. Use this report to detect suspicious user activity.

User Name	Actions
ENTERPRISE\D.Harris	663
ENTERPRISE\J.Carter	44
ENTERPRISE\T.Simpson	21
ENTERPRISE\A.Watson	15
ENTERPRISE\G.Brown	8

3. Keep track of access to archived data

Regularly review a list of all users who accessed data on your archived storage, along with when each access occurred and what files they read.

Access to Archive Data

Shows users who accessed files in your archive storage. A high number of reads may indicate malicious activity. Use this report to detect suspicious activity and exercise security control over your data.

User Name	Reads
PRECINCT34\D.Harris	118
PRECINCT34\G.Brown	5
PRECINCT34\T.Simpson	2
PRECINCT34\J.Carter	1
PRECINCT34\A.Watson	1

4. Detect unusual access to sensitive data

Catch users accessing files with sensitive information they normally don't need and investigate suspicious data usage patterns to ensure data security.

Data Access Surges

Shows users who have accessed sensitive data they almost never accessed before (by default, the inactivity threshold is set to 2 actions). The report highlights previously inactive users who performed more actions within a short period of time (by default, 7 days) than during a considerably longer preceding period (by default, 30 days).

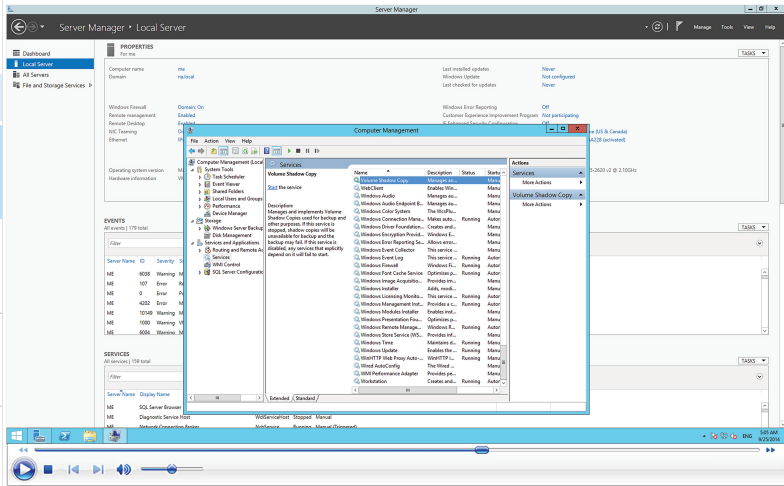
Path	User Name	Attempts
\\fs1\Office\Finance\Cardholders.xlsx	ENTERPRISEJ.Smith	19
http://spenterprise/Documents/Legal/Social Security Numbers.xlsx	ENTERPRISEVG.Johnson	11
\\vmcfs2\Office\Accounting\Budget2016.xlsx	ENTERPRISEJ.Rosenberg	6
\\nf1\Marketing\Backup\Passwords.txt	ENTERPRISEV.D.Harris	2

5. Video record the activity of users

Bridge visibility gaps and spot potentially harmful activities such as the unauthorized use of memory sticks, running of applications that users aren't supposed to run, and other events that are impossible to log.

← Search
WHO
ACTION
WHAT
WHEN
WHERE

⚙ Data source "User Activity (Video)"

🔗 Open in new window


Who	Object type
ENTERPRISEJ.Carter Show video...	Window
ENTERPRISEJ.Carter Show video...	Window
ENTERPRISEJ.Carter Show video...	Window
ENTERPRISEJ.Carter Show video...	Window

About Netwrix




Netwrix Corporation was first vendor to introduce a visibility platform for user behavior analysis and risk mitigation in on-premises, hybrid and cloud IT environments. Founded in 2006, Netwrix has earned more than 100 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

Netwrix Auditor is a visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations and access in hybrid IT environments to protect data regardless of its location. The platform provides security analytics to detect anomalies in user behavior and investigate threat patterns before a data breach occurs.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware and Windows Server. Empowered with the RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises or cloud-based IT systems in a unified way.

More than 160,000 IT departments worldwide rely on Netwrix Auditor to detect insider threats on premises and in the cloud, pass compliance audits with less expense, and increase the productivity of IT security and operations teams.

For more information, visit www.netwrix.com

 On-Premises Deployment Download a free 20-day trial netwrix.com/go/freetrial	 Virtual Appliance Download our virtual machine image netwrix.com/go/appliance	 Cloud Deployment Deploy NetwrixAuditor in the cloud netwrix.com/go/cloud
--	---	--

Corporate Headquarters:

300 Spectrum Center Drive, Suite 200, Irvine, CA 92618

Phone: 1-949-407-5125 Toll-free: 888-638-9749 EMEA: +44 (0) 203-588-3023



netwrix.com/social