

The New Face of Corporate Espionage and What Can Be Done About It

WRITTEN BY

Evan Gibbs

This article was originally published on August 1, 2022 in [Security Magazine](#) and is republished here with permission.

When I tell people that my law practice is heavily focused on corporate espionage litigation and investigations, the typical response is, “Oh, that sounds really cool.” The word *espionage* brings to mind secret agents stealing classified information from tightly-guarded buildings, barely escaping with huge explosions in the background.

And sure, that’s one type of espionage. But there’s another, much more common type happening at nearly every company in the world.

Modern-day corporate espionage is the infiltration or exfiltration of data, documents, and information belonging to one company, individual, or state actor for use by another company, individual, or state actor.

The materials we’re talking about can be secret-sauce-type information. But more often, it’s mundane things like financial data or modeling, operational documents, software coding and algorithms, customer information, and other confidential materials. These materials are sometimes trade secrets, but not always.

Corporate espionage *can* happen via external means — i.e., people outside the organization trying to get insider information using methods such as hacking or phishing. Because of the prevalence and severity of these external threats, many companies’ digital security personnel overlook internal threats.

Internal threats typically involve individual employees or contractors (and often groups of employees or contractors) who are freely given access to sensitive and confidential corporate materials for the performance of their work for the company.

These individuals then download those materials to a personally-owned external drive, usually an external hard drive. People also send company materials to their personal e-mail accounts and upload company data to personal accounts on cloud-based storage platforms. Individuals may even print sensitive corporate materials to avoid a digital footprint. There may not be any ill intent involved or this activity might occur only in the final weeks or days of someone’s affiliation with a company.

In either case, these individuals then go to work for another company that could be a competitor, and the materials

are used on behalf of the new organization. Quite often, sensitive data and confidential documents are distributed to other individuals at the new company. This process occurs far more frequently than most people realize.

How important are internal threats?

In recent years, anecdotal data and national litigation activity reporting indicate a sharp increase in data infiltration and exfiltration by employees and other individuals with internal access to confidential company materials. This is especially true beginning with the onset of the pandemic due to the shift to work-from-home arrangements. In fact, more than [1,300 trade secret claims](#) were brought nationally in 2020. Hundreds of millions of dollars were awarded as damages in 2020 alone.

Unlawful data infiltration and exfiltration have heavy financial impacts on companies whose data is stolen. The damage may not always be readily apparent or immediate, but loss of important confidential materials can erode competitiveness and ultimately impact market share — especially when the materials go to a direct competitor, which is often the case.

There can also be enormous financial implications for companies receiving (whether knowingly or not) materials from another company. Lawsuits seeking double damages and attorneys' fees are common. Companies can face reputational harm if they are perceived as engaging in such conduct. Defending these lawsuits is very expensive, with the bulk of the costs being expended upfront during the preliminary injunction phase.

Given the increase in internal data infiltration and exfiltration and the value of such claims, companies need to take appropriate steps to protect their own confidential materials. And in today's highly competitive and litigious climate, it is equally important that companies take reasonable measures to prevent individuals from infiltrating their systems with data, documents and information from competitors and others.

Below are three key steps companies should take to prevent both exfiltration and infiltration of confidential company materials.

Step 1: Digital Sandboxing

Exiting employees will sometimes download company materials en masse on their way out the door. This often includes materials they did not even use as part of their work for the company. A salesperson might download operational documents; a financial analyst might download customer lists. This is often a function of grabbing entire files and folders from a server and copying them to an external hard drive.

Companies should strongly consider limiting employee and contractor access to only data and materials needed for that person's work on the company's behalf. If there's no business reason for a salesperson to have access to HR files, then access should be restricted accordingly. Doing this limits the scope of company data available for theft and retention by departing individuals.

It's also a good idea for companies to consider blocking USB port access on company-owned computers where possible. One of the most common means of exfiltrating and infiltrating data is via external hard drives, so if USB port access is shut off, the methods by which someone can download or upload data is much more restricted.

Of course, people can still send materials via e-mail to get around a USB port block; however, based on file size restrictions common to most e-mail systems, the amount of data that can be infiltrated or exfiltrated via e-mail is quite limited as compared to an external hard drive.

Step 2: Policies and On/Offboarding

Let's face it: Employees and contractors don't read employee handbooks. Most handbooks are 50+ pages long and only reviewed when there are questions about leave.

Because of this, if a company is serious about putting its employees and contractors on notice that the company takes exfiltration and infiltration of data seriously, there needs to be a standalone document on this issue. Burying the policy in the handbook nearly guarantees it will never be seen.

Instead, companies should give employees and contractors a copy of this policy during the onboarding phase. The policy should be short (one or two paragraphs), be in a large and clear font, written in simple English (not legalese), and generally stand out from the other standard onboarding documents. It needs to unquestionably put people on notice of what is prohibited and require the individual to sign the document, agreeing to abide by its terms.

Companies should also consider including a sentence or two about this in employment offer letters as another means of calling out this issue. Most people read their offer letters carefully, so including some of this information there can further impress upon individuals the importance of this issue.

Departing employees or contractors should get another short document outlining in simple terms what they are prohibited from taking with them and that they could be subject to litigation if they violate those requirements. They should again be required to sign the document, promising not to violate its terms. If exit interviews are done, this issue should be discussed then.

The best way to identify data exfiltration is by forensically reviewing the company-owned accounts and devices belonging to employees and/or contractors — especially those in key organizational positions and those with access to critical company materials. Such forensic analyses must be done close in time to the individual's departure to ensure against a loss of reliable forensic data.

Additionally, these investigations should be conducted by professionals trained in this area. If exfiltration is found or suspected, a thorough investigation should be conducted to assess the best next steps.

Step 3: Buy-in and Training

Another key to preventing infiltration and exfiltration of data and sensitive material is management buy-in. It is imperative that leaders know what activities are prohibited and actively enforce the company's policy on these issues.

It's very common for people to bring materials from another company as a "shortcut" to avoid having to create things from scratch — simply as a matter of convenience. Other times, materials are brought from another company

because the data or documents can help give the new company a real or perceived advantage.

If managerial employees know both what to look for and what to do when they see this type of conduct taking place, it's much more likely that appropriate steps will be taken. This requires specific training for management-level employees on these issues because these problems are often overlooked and misunderstood.

Corporate espionage is far more common than most people realize and is a very real and present threat to company confidential data and materials. Taking the steps outlined above will help organizations reduce the risks flowing from corporate espionage activity.

RELATED INDUSTRIES + PRACTICES

- [Corporate Espionage Response Team](#)
- [Labor + Employment](#)
- [Noncompete + Trade Secrets](#)