EMPLOYEE THEFT: WHY IT’S ONE OF THE BIGGEST THREATS TO YOUR BUSINESS (AND HOW TO STOP IT)

May 2017
When dealing with your company's finances, you likely work hard to not only ensure your books are balanced, but also pull in as much profit as possible every year. To save money and keep accurate records, you pay close attention to various areas in your business, like discounts on wholesale supplies, routine maintenance of expensive equipment, and the pricing of your products or services. But your biggest threat to your year-end profit and reports may actually be within your organization, as employee theft is one of the most rampant and common ways businesses lose money, assets, and even their reputations.

For years, various outlets have reported one in three businesses will fail due to employee theft. On average, 75% of employees will steal at least once in their time of employment, and their theft is 15 times more likely than nabbing by external people.

Employee theft is so prevalent that an independent study from 2013 by forensic accounting firm Kessler International of over 500 businesses discovered 95% of employees are likely to steal from their employers. This figure is up 16% from Kessler’s previous study from 1999, a disconcerting increase considering the problem of employee theft costs businesses thousands to millions of dollars a year. Kessler attributed the rise of employee theft to factors such as employee misuse of assets and the penchant for younger employees, boasting a sense of entitlement that they’re owed more than they’re given, to have less honesty and integrity than previous generations of workers.

One example of just how much money companies stand to lose due to employee theft comes from internationally-renowned Swedish home brand Ikea. Back in 2008, a 24-year-old man named Suraj S. Samaroo was working in an Ikea call center in the Baltimore, Maryland area. His duties included handling complaints and returns from the retail giant’s customers; instead, Samaroo used a fake name and address, his bank routing number, and the legitimate records of Ikea customers to issue more than $407,000 worth of refunds to himself over the course of a year for items which were never actually returned.

“He would do that at a steady clip - two or three times a week - every week for a year,” said the case’s prosecutor, Adam Lippe, to The Baltimore Sun. “The money was sucked out of whatever big pot of Ikea gold there is and transferred to his bank account.” Samaroo, who had used some of this stolen money to buy himself an Infiniti G35X, was eventually arrested and charged with theft and theft scheme.

While it might seem Samaroo was clearly in the wrong, his defense attorney T. Wray McCurdy's stance on Ikea's negligence is what all businesses should be concerned about when it comes to employee theft: “It makes you stand back and wonder how he had access to such a scheme in the first place. Where are the supervisors? Are there any? I’m not saying he’s not responsible for the loss - he is - but ... it makes you shake your head that a major corporation doesn’t have enough checks and balances to prevent something like this.”
What Counts As Employee Theft?

In order for any business to avoid the same problem Ikea encountered with Samaroo, as well as implement a proper checks and balances system, they need to realize just what exactly employee theft is and how it affects their bottom lines. While employee theft is, in many ways, straightforward to define, there are a few different types you should be aware of in order to better understand the relationship between the theft and the way it hurts your company:

**Time Theft**

Employees who misuse company time in any unapproved manner are stealing your time. In Kessler’s 2013 study, at least 30% of employees admitted to falsifying time- or schedule-related documents at work. One example of this type of theft comes from Joseph Winstead, a United States Postal Service worker who fabricated court paperwork and avoided his job for 144 days by pretending he was on jury duty. This time Winstead wasn’t working earned him/cost the USPS over $31,000.

Theft of time can also include when employees use company assets for unauthorized personal pursuits, interests, or business. For example, if one of your employees were to use a company car to go to lunch with a friend (not for business purposes) or get on Facebook for thirty minutes on a company computer, these actions could be considered time theft. In fact, around 80% of Kessler’s survey respondents admitted to using company computers or phones for personal reasons.
Asset Panda has definitely impacted our bottom line in that we are now able to see the whole picture as it pertains to assets, all in one place. “

Money Theft

As seen above with Samaroo’s example, employees are not above stealing cash or funds directly from their employers. Employees can conduct billing schemes, where they set up a fake vendor account for themselves and then pay that “vendor” for nonexistent products or services. Payroll schemes, on the other hand, are created when an employee alters timecard information to earn more money than time actually worked, or write checks to fake employees.

Your employees could also try to set up an expense reimbursement scheme, where they claim expenses for items which were never actually incurred or used for business purposes. Finally, embezzlement (the theft or misuse of funds placed in someone’s trust), fraud (an intentional deception used to gain personal or financial gains, as exemplified by Winstead’s case above), and larceny (theft of personal property) are also common forms of employee stealing which directly result in a financial loss for companies.

Asset Theft

When an employee steals an asset, item, or piece of inventory owned by your company, it is considered asset theft. Kessler found 52% of survey respondents admitted to stealing some sort of company asset from their employers. The most common items were office or building supplies, including pens, notepads, toilet paper, and even printer toner (as employees would print off personal documents at work). A German caretaker, for example, stole 20 tons worth of office supplies over the course of 30 years. However, some employees will risk even more expensive pilfers, including a former Tiffany’s executive who stole 164 items of jewelry, worth about $1.2 million.
While some businesses may not mind if their employees take home a marker or notepad every so often, the problem becomes more threatening when larger, expensive items are considered, such as computers, mobile phones, or even company cars. Employees can also steal the products or services your company creates for your customers; for example, an employee could nab a physical item from your warehouse shelves, or illegally download a copy of your company software for personal use without paying for it. Around 35% of respondents in Kessler’s study admitted to pilfering products or services.

**Data Theft**

Finally, employees can also steal company data or information directly from under your nose, despite having signed a contract or NDA prohibiting such actions. Employees can take and use all kinds of data for personal gain, including company secrets, proprietary information, customer information, marketing data, internal processes, and systems, etc. While Kessler discovered only 18% of employees had ever stolen company information, this loss can be one of the most detrimental to both a company and its customers.

As an example, in 2008 the UK-based Colchester University Hospital had to fire one of its more dedicated managers because, while on vacation in Edinburgh, his company laptop was stolen from his locked car. The thieves who broke into the vehicle were able to bypass the computer’s security and steal the identities and information of several thousand hospital patients. The loss of patient data meant the hospital’s reputation was tarnished, as was the safety and personal information of its patients.

**How Much Does Employee Theft Cost Companies?**

The common thread across the different types of employee theft is they all cost businesses far more each year than is necessary. Estimates for how much businesses lose each year to employee theft range greatly from industry to industry, but the Association of Certified Fraud Examiners (ACFE) determined in a 2016 report that companies worldwide lose roughly $6.3 billion to fraud alone. The Association also estimated businesses lose roughly 5% of annual revenues to employee theft and fraud, with a median loss of $150,000 per organization.

The ACFE’s study, however, only covered around 2400 cases of employee fraud across various industries from January 2014 to October 2015. When you consider the losses from employee theft in specific industries, the situation becomes dire. For example, a 2015 study from Retail Knowledge discovered U.S. retail companies on average lost $60 billion; 38% of this shrinkage was attributed to employee theft. Additionally, retail employees tend to steal more often than customers at a rate of 43% vs. 37%, a problem which cost the retail industry an average of $18 billion in 2013 alone.
Here are some other facts about how much employee theft affects businesses financially:

- In the ACFE’s study, 6.6% of all employee fraud cases were in the healthcare industry, causing these businesses an average median loss of $120,000 per case. Healthcare employees were most likely to try billing schemes, expense reimbursements, and general corruption schemes.

- Construction companies, while boasting a significantly smaller percentage of cases in the ACFE study at 3.6%, stands to lose far more per case of employee theft or fraud at an average median loss of $259,000. And in a 2014 Equipment Theft report, the National Insurance Crime Bureau and the National Equipment Register determined the construction industry is at risk of losing up to $770 million per year due to theft, employee-conducted or otherwise.

- Government and public agencies seem to be the most at risk for employee theft and fraud, due to their size and large employment numbers. At 10.5% of all ACFE’s reported cases, government organizations were the second most likely type of organization behind banking and financial services to experience employee theft and fraud, with median losses of $133,000.

- Educational institutions are also not immune to employee theft, though, on a per-case basis, this industry boasts one of the lowest median losses of all at $62,000. However, the ACFE noted educational organizations and businesses reported a fairly high number of cases on average at 132 (around 6% of all studied cases) during the duration of the report’s timeframe.

- Unfortunately, non-profit organizations and churches deal with a higher average median loss per employee theft case than educational organizations do, at $82,000 per case. These industries, however, reported a significantly fewer theft and fraud cases during the study than any of the four previous industries mentioned above in just 52 cases (2.4% of ACFE’s total samples).

**Why Does Employee Theft Go Unnoticed or Unreported?**

Despite the immediate problem of employee theft, the topic is not always at the forefront of business owners’ minds. In fact, some might even ignore it, or decide not to report it at all. This lack of attention to or reporting of employee theft happens for several reasons:

**An Improper Hiring Process**

When businesses fail to perform in-depth background checks of potential employees, they put themselves at risk for hiring questionable or disreputable people who may not hesitate to steal from the company in the future. In the same vein, many business owners fail to see the importance of hiring methods like character tests or ethical questioning; unfortunately, if these measures were implemented, companies may start to see fewer disloyal and unscrupulous employees stealing from them.
A Lack of Internal Controls

The most common reason employees are able to nick items from their employers without notice is because the company doesn't have proper internal controls in place, including asset tracking and management solutions, security measures, routine audits/reviews, surveillance, etc. Poor internal controls were the most-cited reason (29%) in the ACFE’s report for missed occurrences of theft, with an override of controls following closely behind (20%).

A Shortage of Proper Reporting Channels

The ACFE discovered many of its studied employee theft cases were ultimately apprehended thanks to tips, which accounted for at least 39% of cases. However, non-employees like customers and vendors are the most common tippers at 40%, which implies employees may not have the proper or safest channels for reporting the wrongdoings of their colleagues. For example, businesses which boast hotlines were 47% more likely to catch schemes vs. companies without hotlines at just 28%.

A Sense of Loyalty/Connection to Employees

Some businesses can be blind to the stealing inclinations of their employees if they have emotional ties to them, one of the top reasons only 16% of small businesses report an internal theft. This sense of loyalty to your employees likely increases with how long they have worked in your business, though that length of employment actually increases their chances of stealing. In fact, in the ACFE’s study, the average length of reported employee fraud cases before the perpetrators was caught was 18 months.

A Fear of Bad Reputation/Press

While small businesses may not report employee theft because they have, among other reasons, emotional ties to their workers, ACFE discovered 40.7% of companies who were victim to employee theft and fraud didn't want to report the issue to the police or law enforcement due to a fear of bad publicity. This fear beat out other reasons quoted for not reporting a theft, including sufficient internal discipline and private settlements.

A Distrust of the Legal System

For small businesses in particular, who stand much more to lose compared to a larger business when the average median loss per employee theft is $150,000, reporting an employee’s stealing is often not worth the time or money a court case would inflict on top of the already-stolen losses. Small businesses have also cited a lack of trust in law enforcement members who may not care about or understand business intricacies, or who may be too busy with other enforcement needs to do anything other than write up a theft report.
How Can Companies Protect Themselves?

By now, you can see just how commonplace but dangerous employee theft is to your business. You stand to lose thousands, if not millions of dollars, per year depending on your particular industry. You could also end up short on assets, products, or inventory, as well as lose hours upon hours of what could have been productive work time thanks to employees pursuing their own interest during work schedules.

As you probably noticed above, several procedures were already outlined which companies can implement to help deter employee theft and protect themselves from similar heists in the future. These are some of the most common and highly-effective ways to reduce or eliminate employee theft from your organization:

**Implement More Thorough Background Checks**

The more in-depth, qualitative background checks you can conduct on potential employees, the more likely you are to avoid hiring ones who have a record of bad behavior, specifically in terms of stealing. In addition to pulling legally-available public documents on your potential hire, consider calling their previous employer(s) to discuss their work ethic and history.

**Conduct Personality/Character Tests**

You can try to determine the integrity of a potential employee by asking them to complete a personality/character test or ethics questionnaire as part of their interview process. Their answers to the tests will help uncover any qualities which could be associated with thieving and dishonest tendencies.

**Remove the Reasons for Stealing in the First Place**

Back in 2001, management and workplace efficiency researcher Gary Latham once helped a sawmill save around $1 million in equipment years by eliminating the thrill of stealing, which spurred mill’s employees. He did this by making all the mill’s assets free and creating a library-style check-out system, so there was no need for employees to take anything unauthorized anymore. Latham also instilled an “amnesty” day, where the mill’s management allowed employees to return items they’d stolen free of punishment.

**Increase Monitoring Measures**

Your business can also decrease the possibility of employee theft by implementing more comprehensive monitoring solutions. For example, video cameras can be installed in the office or store, and GPS chips can be installed within the valuable equipment. You should also consider setting up an email notification system for monitoring expenses, so if an employee were given a business charge or credit card and started using it to buy unauthorized purchases, you would be aware of the situation immediately.
Perform Routine, Frequent Audits and Reviews

Using programs or having an effective auditing review process in place will help companies better and more quickly detect unwarranted changes to ledgers, asset logs, company data, etc. ACFE’s study discovered 94.5% of employees who stole tried to cover their tracks, mostly by creating or altering physical documents; this situation would happen far less if companies routinely inspected their physical assets (or even moved them to the cloud altogether).

Set Up a Robust Asset Tracking and Management Solution

According to the ACFE, asset misappropriation was involved in the majority (83%) of employee fraud cases. Therefore, using a robust asset tracking and management solution can help you deter employee theft, as well as put the control of your business back in your hands. Such a system will allow you to not only better organize your physical and digital assets, but be able to track in real-time where they are and if they’re being used appropriately.

How Asset Panda Can Help You Prevent Employee Theft

While there are a lot of asset tracking and management software options on the market, Asset Panda is one of the only solutions which is flexible enough to work with your goal of deterring employee theft. Here are a few reasons why using our software can alleviate your concerns about internal theft and dishonest employees:

- With Asset Panda, you can apply different security levels and role-based access to various users. This feature means you can provide high levels of access to your asset information only to those reliable employees who need such access. All other employees can be assigned lower levels of access, making it harder for them to both alter company records and steal from the business without being noticed.

- Our software utilizes secure servers from one of the most trusted digital security companies in the world. What this feature provides you is the peace of mind of knowing both outside forces and employees can’t steal or destroy your data to try to cover their tracks.
Asset Panda’s software works in real time, updating every single time an employee scans in a returned laptop or checks out a company vehicle for a business trip. When you keep your assets up-to-date, it’s much harder for an employee with a penchant for stealing to swipe anything from under you without you noticing.

Our asset tracking solution is customizable, meaning you can set up your own processes, systems, tags, and more. While this capability might seem like a minor benefit, customizing your asset tracking system ensures not just the accuracy of your asset and inventory information, but also reduces the chance an employee can get away with stealing a particular item because you’ll know exactly what’s missing and can search for it (for example, you’re more likely to track down a missing 14” Dell laptop with 4GB of memory purchased and a specific UPC code, but it’s much harder to figure out who stole one laptop which had no specifications noted in your asset system).

Asset Panda’s mobile app boasts a barcode scanner, which provides you the ability to scan and automatically populate required and optional information for new and old assets alike into the system. The ability to quickly and accurately scan your assets reduces the chances of an employee stealing them before they’re saved into your database. The barcode feature also makes it harder for employees to alter asset information without permission.

With our software, you can also be alerted by email anytime the status of an asset change. This communication, of course, is one of the easiest ways to determine whether or not an employee was acting with your permission in regards to that asset or is trying to steal the asset.

Finally, Asset Panda helps you save money simply for the reasons outlined above, all of which make it harder for employee theft to go unnoticed. The fewer assets you lose to employee theft, the more money you save your business in the long run. Overall, you’ll be able to properly balance your books, conduct audits, and provide accurate financial reports without having to worry about accounting for stolen items.
One Asset Panda customer, in particular, has seen positive impacts on its bottom line. The Jefferson Parish Sheriff’s Office (JPSO) Crime Lab in Louisiana had a lot to lose when its technology hardware was constantly being shuffled around to different employees, but the Crime Lab’s IT department wasn’t able to track them with a central tool other than Excel. This problem was a major concern to the JPSO, considering it receives funding from various sources. After implementing Asset Panda, the department experienced financial benefits:

“Now we can track the funding source per asset, which has been an invaluable tool due to the customization Asset Panda offers. That being said, the built-in barcoding, customization of the software and the implementation of the mobile app are all features that we have found especially useful. The mobile app, coupled with the barcoding allows me to have all of the assets information at my fingertips simply by scanning, whether it is from my iPhone or iPad. Asset Panda has definitely impacted our bottom line in that we are now able to see the whole picture as it pertains to assets, all in one place. Instead of different areas trying to manage their respective assets, they are now centrally managed on an incoming and outgoing basis.”

Danielle Shirk, Laboratory Service IT

If you’re interested in seeing more of what Asset Panda can do to deter employee theft, sign up for a free, 14-day trial, or give us a call at 855-898-6058.
About Asset Panda

Asset Panda, the most powerful, yet simple to use free asset tracking software in the world, enables clients to track their IT assets exactly how they want, and from the mobile devices they already carry. The platform may be accessed either online or via free mobile iOS and Android apps that sync with the cloud. The apps include a mobile barcode scanner, so there’s no need to purchase a separate handheld barcode scanner. Users can add voice notes, videos, documents or photos to the asset’s information. The tool allows users to view check-in/check-out status, GPS location, lease/purchase information, complete maintenance history, insurance information, and the depreciation and inflation calculations your accounting and compliance teams require. Companies of every industry sector and size – including some of the world’s biggest brands – have chosen Asset Panda to help them manage millions of dollars' worth of vital assets.

Schedule a demo: assetpanda.youcanbook.me
Tel: (855) 898-6058
Email Us: info@assetpanda.com

Headquarter Office: 3001 Dallas Parkway, Suite 580, Frisco, Texas 75034

www.assetpanda.com

© 2017 Copyright Asset Panda