

How can you deal with employees who spill company secrets?

hrgrapevine.com/content/article/2020-04-06-how-can-you-deal-with-employees-who-spill-company-secrets



When it comes to the workplace, employees can ‘make or break’ a business in regard to the information that they know and hold. This may be why companies such as KFC and Coca-Cola have notoriously been known to keep their famous recipes close to their chests. In fact, KFC’s 11 herbs and spices are allegedly only known by two people in the world and they are not allowed on the same plane at any time together. Some may say that is extreme, but this demonstrates just how important it is so safeguard company information.

While many businesses do their best to keep their secrets safe, some employees from well-known organisations have been quick to reveal all to the public. In fact, research has found that more workers would be willing to sell company information than first thought, as data from a cyber security firm revealed in 2019. Deep Secure’s *What is the Price of Loyalty* report discovered that a quarter of staff members would be willing to sell corporate information for just £1,000.

Whatever the reason may be for leaking corporate details, according to a poll by security specialist Ipswitch, many employees just aren’t taking company security seriously. 50% of employees admitted to carelessly sending secret information via email. In addition, 25% said that they had sent confidential files to their personal email addresses, with the intention of using the information as an asset for a better position at a competitor company.

It, therefore, may come as no surprise that last year saw an employee from bakery firm Panera Bread expose how the company prepared its famous mac and cheese dish. After sharing a video detailing the preparation of the dish on social media, which garnered six million views, employee Brianna Ramirez was dismissed from her position at the bakery.

Similarly, a former Disney employee also shared a video last year where she spilled an abundance of corporate secrets including one that explained the reasoning behind why Animal Kingdom bathrooms were the only ones with doors – to allow guests to hide in if an animal was to escape. With this in mind, what can encourage employees to spill company secrets?

"A great deal of 'damage control' is about getting ahead with messaging both internally and externally"

Why do employees spill secrets?

In a UK study of 2,000 workers, Egress Software Technologies found that 24% admitted to email misuse and purposely sharing sensitive business data over email, but corporate secrets can be revealed in a variety of ways for different reasons – malicious conduct, social media slip-ups, carelessness and even coercion can cause an employee to share too much information. For example, a disgruntled employee may be unhappy with the way their employer treated them or they may wish to get some sort of revenge on a co-worker who was bullying them.

This is something Martin Kirke, Non-Executive Director, Coach and HR Consultant and former Group HR Director at the Post Office, alludes to. He shares: "In my experience there's a wide range of reasons. Revenge against a bad line manager or a decision that's been made. Sometimes it can be naivety and getting carried away with social media. It can also happen where the culture is not inclusive and employee engagement is poor."

"If you suspect an employee is about to disclose confidential information, consider seeking a court order (injunction) that would prevent the employee from disclosing or using that information"

Damage control

For Bobby Davis, Chief People Officer at Almarose Hotels and Resorts, she knows all too well how important it is to keep company information close to her chest as she previously worked within the British Army, where she in her own words 'would have gone to prison if I had revealed such information during military service'. However, she believes there is a certain amount of damage control an employer can work on, both internally and externally, if a secret is revealed.

"A great deal of 'damage control' is about getting ahead with messaging both internally and externally," she tells *HR Grapevine*. "Internally, there is a need to mitigate and remind people of the severity and impact. Externally, it may be necessary to be transparent and make a press release." She adds that if company information is ever released unlawfully, employers should consider putting in place systems and processes in order to safeguard information, so that employees do not freely have access to it to share.

She adds: "As well as making a priority of taking control of communication and messaging, it is also necessary to consider systems, controls and processes. There perhaps needs to be a review/evaluation piece to understand how the situation came to pass in the first place. Is it purely human or can action be taken in terms of systems, controls, technology to prevent a repeat?"

Can law be enforced?

KFC's recipe and the Coco-Cola formula are considered trade secrets and can be protected in the UK either through a common law action for breach of confidence, or a breach of contract action when an NDA exists or can be implied, reports Harper James Solicitors. Trade secrets are protected without registration, that is without any procedural formalities. However, to qualify for protection in the UK through common law, certain elements need to be present to constitute a breach of confidence, including that it must have been an unauthorised use of the information and that there must be an obligation of confidence.

In addition, Roberta Pasemko, Associate at law firm Lewis Silkin, shares that employers should consider seeking a court order if they suspect an employee is acting unlawfully and looking to divulge secrets. Pasemko explains: "If you suspect an employee is about to disclose confidential information, consider seeking a court order (injunction) that would prevent the employee from disclosing or using that information.

"Alternatively, if the information has already been disclosed, an employer can seek an order for delivery up, a prohibition on further use and other remedies such as damages or an account of any profits made. If you have a suspicion but no evidence, investigate and, if appropriate, discipline the employee in accordance with company policies."

This is something that Michael Hatchwell, Partner at Child & Child, also agrees with, but warns that employers should be aware of the costs involved. He adds: "Protecting confidential information will also usually require court action. This can be an application for an injunction against an infringing person or a claim for damages for disclosure. Such actions may have a good chance of success. But action is expensive and so when asked to explain the value of such provisions a legitimate response is to say the cost of enforcement."

"Cultures which are open and encourage engagement are more likely to identify issues before they blow up"

Working on prevention

While introducing workplace policies and clauses may help to deter employees from divulging company information, Davis believes this only scratches the surface. Instead, she urges employers to focus more on company culture and make everyone aware that it is their responsibility to protect trade secrets in order to prevent them from sharing with the public.

"It's not just the responsibility of the CEO, leadership, information governance – everyone has to play their part [in protecting secrets]. [Employers should] educate everyone in the organisation on the importance and value of company information and helping them appreciate that it is as much of an asset as they are the company's products are," she comments.

"As a result of the education, strong policies and procedures can be established which aren't onerous or punitive but look to support people doing their jobs well and not 'dropping the ball' when it comes to information security."

Meanwhile, Pasemko also placed a key importance on setting out clear workplace policies for employees to follow if employers are to safeguard their trade secrets appropriately. Pasemko continues: "Prevention is better than cure, especially when it comes to protecting trade secrets and confidential information.

"Employers should set clear boundaries at the outset of the relationship [which] express contractual clauses and robust workplace policies, including a social media policy, that addresses what information the business considers confidential (while avoiding long, generic lists) and how that information should be treated. The distinction between less sensitive information, confidential information and trade secrets can be hard to digest, so bring policies to life by offering practical training sessions."

Culture shock

Ultimately, if an employee feels disgruntled, they may act out and take revenge by sharing company data, which may not easily be stopped by an employer. However, if employers encourage an open culture where staff can come forward about their issues, the desire to leak secrets may diminish. This is supported by Kirke, who tells *HR Grapevine*: "Cultures which are open and encourage engagement are more likely to identify issues before they blow up."

The implication being if employers aim to implement all of these factors, from an open culture to clear workplace policies, organisations may be able to sleep easy at night knowing their trade secrets are protected.