**News**

# Misuse of Confidential Information – Are You Prepared?

**Date:** March 20, 2012

An employee's misuse of confidential information housed on computers or electronically can expose an employer's business to serious risk of harm and potential liability. Improperly managed, these situations can create a crisis: witness Bank of America and the WikiLeaks threat.

Hicks Morley has been successful in assisting clients who have had their confidential information misused by employees. We have also had success in advising clients who have hired employees that brought confidential information of a third party into the workplace without our clients' knowledge. This article discusses how an employer can respond if faced with these situations.

## Employee Misuse of Computers

Employee misuse of computers arises in a variety of circumstances. For example, an employee may be using his work computer to send information to competitors, or to send emails containing confidential information belonging to the employer to his home; alternatively, an employee may be using the computer to run his own business, or even for illegal purposes.

In all of these cases, immediate steps must be taken to secure and preserve key evidence such as the employee's computer hard drive and Blackberry and to ensure "chain of custody." It is critical that this be done quickly and properly to avoid possible allegations that the evidence has been tampered with or otherwise tainted. Something as simple as reviewing the hard drive can change the underlying metadata, potentially undermining the usefulness of that information as evidence. In many instances, it may be advisable to retain an outside forensic expert to ensure that proper steps are taken. Not only do outside experts know how to deal with such evidence, they are able to provide independent expert evidence on these matters in the course of subsequent litigation, if necessary.

Once properly secured, the hard drive should then be imaged. This is akin to taking a photocopy of the hard drive. This imaged hard drive allows the computer expert to conduct searches without jeopardizing the original hard drive and metadata. Keyword searches can then be conducted and a spreadsheet summarizing all hits of keywords can be created. This allows the employer to pull relevant documents to determine if the employee has committed wrongdoing. It can also be determined whether information has been uploaded to other devices. We have seen experts who have pinpointed the serial number, type of device and the exact date and time the information was uploaded.

## Seeking the Return of Confidential Information

After doing a forensic review, an employer may discover the employee has uploaded information relating to a segment of the business or an important client, or has emailed thousands of employee personnel files or the confidential information of vendors to his or her home account, for the purpose of gaining leverage in a dispute with the employer.

While an employer may apply to the courts for an order for the return of the information, this can be costly and time-consuming. Often courts do not move fast enough to allow an employer to avoid the harm, and other means must be found to protect the employer. For example, sending a detailed letter setting out the findings of the forensic review, including what was uploaded to specific media devices, when, as well as what information was sent by email, is often an effective, and comparatively inexpensive, measure. This letter may also outline steps the employee took to hide their wrongdoing, such as deleting emails, and demand that the information be returned and be irrevocably deleted. Often when faced with the reality that they have been found out, the employee will co-operate to minimize potential liability.

At times, it may still be necessary to take additional steps such as initiating a claim, or hiring a private investigator to find out other details to determine if the employee can be trusted.

## Misuse of a Third Party's Confidential Information

Imagine receiving a phone call from legal counsel for a competitor stating that they have proof that your new employee has wrongfully taken confidential information from that competitor. Worse still, imagine that you are advised that there is clear evidence that the confidential information has been uploaded onto your company's computer system. You may now face a lawsuit and an injunction, not to mention potential damage to your business reputation.

There are several lessons to learn here.

First, as a proactive measure, an employer should have a new employee acknowledge in their employment contract that they do not possess any confidential information belonging to their former employer, and undertake not to use any such information in the course of their new employment. If there are any questions relating to whether their former employer's information can be used, the employee should agree to raise the issue with the new employer beforehand. Finally, the employee should acknowledge that their employment may be terminated for cause if the agreement is breached in this regard.

Second, if it appears that the employee has wrongfully taken confidential information, an employer must take proactive steps to minimize any potential liability and to establish that it has acted and will continue to act in a trustworthy manner to protect the legitimate interests of the former employer. A failure to do so may result in the court feeling compelled to intervene and take measures to protect those interests. This could include such measures as the court ordering a forensic audit of the employer's computer system by an outside expert, resulting in significant business disruption and cost to the employer.

These steps could include:

- seeking to negotiate a co-operative process with the former employer's counsel to ensure that all confidential information is returned and deleted;
- getting the employee to confirm what was taken and stored on the company computer system; or
- hiring a forensic computer expert to return the information, ensure it is irretrievably deleted and swear an affidavit to outline the process followed, and confirm that he is satisfied that everything has been irretrievably deleted.

It is important for any process employed to be transparent and replicable. If necessary, the employer must be prepared to satisfy the court that all reasonable steps have been taken to undo any wrong committed by the employee, and that no further measures are needed or warranted to protect the interests of the former employer.

## Conclusion

The ability to store and transmit vast amounts of information electronically offers unique business opportunities for companies; but it also poses some serious risks. It is important that employers be aware of these risks and be prepared to manage them.

For more information, please contact your regular Hicks Morley lawyer.