

IT breaches: a firm's legal recourse

24 June Business Times

By Elaine Tan, Assoc.
Director, Amica Law LLC

ELECTRONIC communications have transformed the face of business. Company records and vital information such as business transactions, sales and purchases, business operating expenses, employee wages and financial statements are maintained electronically instead of being stored in large volume of paper records.

The widespread use of electronic communications brings with it concerns over the security and integrity of such electronic records. This article examines some of the options that are opened to a company if the security and integrity of its electronic records have been breached.

Breach by an employee

Many employment contracts contain a clause that requires an employee to maintain confidentiality of company records and to always act in the best interest of the company. During the period of employment, if a breach is committed by an employee, the company can press for damages for breach of his employment contract and/or for breach of his obligation of good faith and fidelity to his employer.

Regardless of whether the employment contract contains a confidentiality clause, the company can sue its employee for breach of confidence if the following conditions are satisfied:

- The company must show that the information in question is indeed confidential;
- The information must have been imparted from employer to employee under a circumstance where confidentiality is expected/obligated; and
- There must be some evidence to show that the information has been used or disclosed to third parties without the company's consent, or that unauthorised use or disclosure is likely.

In cases involving a breach of confidence, a company would usually seek, among other remedies, a judicial order to prevent further disclosure or use of such confidential information. In certain circumstances, it is possible also for such a judicial order to extend to third parties, for example, a current employer of the former employee.

Computer Misuse Act (CMA)

Whether the breach is committed from within or outside a company, the provisions of the Computer Misuse Act (CMA) could apply. The CMA criminalises acts related to the unauthorised access and use of computers and computer data.

Offences under the CMA are punishable with fines and/or imprisonment. The fines imposed depend on the type of offence committed and are likely to be higher if damage is caused to a company's computer systems. In relation to this, subsequent offenders will face enhanced punishment under the CMA. Higher fines and longer imprisonment sentences apply if the computer qualifies as a 'protected computer'.

Any unauthorised modification, interception and obstruction of a company's computer materials or services are also offences under the CMA. For example, sabotaging a computer programme before leaving the company by secretly setting password protection within the programme that prevents the company from being able to check, modify or upgrade the system could amount to an unauthorised modification or obstruction of computer services.

Finally, it is an offence under the CMA to disclose one's access code (such as user-id and passwords) of any programme or data to other people without the company's permission. Companies are advised to include a clause in the company's employment contract or in their IT Use Policy to remind employees not to disclose their access codes to other people.

Breach by third parties

If a suspected breach has been committed, it is advisable to make a report to the police who will then investigate your complaint. If warranted, a criminal charge will be levied against the offender and the state will have full conduct of the criminal prosecution of the offender.

In the criminal prosecution of an offender, the CMA empowers the Court to make an order for compensation for any damage caused to one's computer, programme or data as a result of the offence. However, orders for compensation is rare and often, if a company wishes to claim against the intruder or offender, the company would have to commence a civil action against the offender.

The unauthorised access to a company's electronic records can amount to trespass, that is, wrongful interference with property. Often, if a conviction has been secured under the CMA, it would be easy to show that the elements of trespass had occurred. The company could seek damages and legal costs.

If a company's database and electronic records had been reproduced, the company can take further legal action for copyright infringement.

Conclusion

The above is not a complete list of options and remedies that are available to a company in the event of breach of the security or integrity of its electronic records.

An ounce of prevention is better than a pound of cure. Implementing the appropriate security measures will help SMEs safeguard their business.

The writer is an IT committee member of the Law Society of Singapore and works for Amica Law LLC

This article first appeared in The Business Times on 24 June 2008 and is reproduced with the kind permission of Singapore Press Holdings.