

COMPU-CRIME COSTS R40BN

Problem is rife and growing at alarming rate, warns expert

White-collar crime, of which computer hacking and tampering forms an integral part, is one of the fastest growing crimes in South Africa and is costing the economy an estimated R40-billion a year, according to Business Against Crime.

A key aspect of computer-related crime is the malicious tampering with computer data by disgruntled or dishonest employees.

Losses totalling many millions of rand are notched up every year, as was evidenced recently when the Edcon group of companies was "hacked" and a virus planted on the network that caused a loss of almost R20-million.

Corporate lawyer Michael Judin says the problem is rife and growing at an alarming rate.

"Because there is virtually no foolproof way of stopping a determined employee who wants to do harm to his employer; it is essential that a range of information technology systems be put in place to track the electronic movement of each and every employee," he says. "This includes having access to their e-mail and keeping a watchful eye on their activities on the Internet."

Michael Silber, of the firm Michalsons Attorneys, specialising in information and telecommunications technology (ICT) law, says devising plans and strategies to prevent data loss was vital.

"It is essential that companies become aware of the scope and magnitude of the problem and that they take appropriate precautions to protect themselves.

"In 1999 an Edgars employee introduced a computer virus into the company's mainframe. They suffered losses totalling some R20-million," he said.

The virus spread through the group's stores across the country, damaging the computer network. The worst day was Saturday, May 15 1999. The virus caused a massive computer crash and sales had to be entered manually.

A forensic investigation found a trail that led back to the employee, who was subsequently found guilty on charges of malicious damage to property because no laws existed at the time that specifically gave protection to data or related to computer-specific crime.

This has been remedied by two new pieces of legislation: the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002 and the Electronic Communications and Transactions Act 25 of 2002.

This makes it possible for employers to keep a much closer look at what their employees are up to, including the tracking of their Internet and e-mail activities as well as enabling them to put written policies in place governing the handling and protection of electronic data.

Gusti Coetzer, founding partner of executive headhunting firm Leaders Unlimited Korn/Ferry International, says everybody from the CEO to the tea lady are potential suspects. "Often the security on company networks is so low that anybody who wanders into an office has access to the entire network," she says.

A large percentage of top companies who use her company for executive searches have expressed concerns and, as a result, there has been a booming demand for network security specialists who could make individual computers and networks more secure.

Judin, who has dealt with numerous instances of employee fraud and sabotage, says the biggest threat to a company was the departing employee. "It is of the utmost importance that a disgruntled employee - irrespective of his or her rank - be banished from the office as quickly as possible. At least restrict access to the company network by changing passwords or withdrawing electronic permission to access sensitive databases."

Coetzer says the Edcon case was a shining example of what a disgruntled employee could do.

"Deleting a company's address book or their client list - or even a portion of it - can have far-reaching consequences and has on occasion been responsible for companies failing," she says.

Silber believes the problem is far more widespread than most business people realise. "While the deletion and destruction of data is undoubtedly a major problem, an even bigger problem is the theft of sensitive information from employers.

"Whole databases containing sensitive customer information are stolen and sometimes offered for sale to a competitor or the thief sets up business for himself, using this information to get his or her business off the ground."

Companies have to have effective whistle-blowing policies in place so be that honest employees can blow the whistle on their crooked counterparts, Judin says. "Physically tracking the movements of employees through various parts of an office at complex is also an effective counter-measure. The system will immediately show which employees accessed an office in the small hours of the morning."

Judin says there is a growing trend for employees to offer information for sale to companies in direct opposition to his employer. "The amazing thing is that some companies would actually offer these individuals a job based on the value of the information they bring with them. They tend to forget that if he did it to his previous employer he could do exactly the same thing to his new employer."

Signs of spying include enquiries by strangers on unreleased information, competitor knowledge of your business, getting beaten on tenders continuously by is the same company and theft of confidential material. Judin says the current trend showed both an increase in volume and in the severity of IT-related sabotage.

*For more information contact Gusti Coetzer of Leaders Unlimited on 011-722-1600. Visit www.internet.org.za for full text of the relevant legislation.

*The above article appeared in *The Star Workplace* Monday, August 28, 2006.