Tough on the causes of crime

Tracking insider computer crime is hard enough. But proving guilt can be even harder.

"We're a lot like undertakers," says Cliff May, a computer forensics specialist at IT security company Integralis. "People only call us when they've got a problem." May has been working in computer forensics for 15 years, and during that time, he says, he has developed a deep understanding of the potential threat to businesses posed by their own employees: "In any organisation, there are people from all walks of life, with debts, gambling problems, jealousies." Given the opportunity, he says, some of those people may use their employers' systems to commit fraud or other crimes.

The criminal activities of hackers are widely recognised, and most organisations now install firewalls and anti-virus software to mitigate the threat posed by them. Little attention, however, is paid to the prevention and detection of computer crime from within the organisation – although, May argues, it is potentially a far greater problem. "It's much easier for someone internal to damage systems than for a hacker [to do so]," he says.

It is also much more costly. According to figures from the Computer Security Institute, an internal IT attack typically costs a company over four times as much as an external attack. Furthermore, according to government watchdog the Audit Commission, most corporate fraud is committed by insiders. The average loss to a company resulting from IT fraud, it says, currently stands at some £36,000. Even if there is no actual theft, the damage caused by IT abuse to a business and its relationships with customers, partners and employees can be very real.

The first priority for any company is to put in place preventative measures, says Paul Vissilis, head of risk services at security consultants the NCC Group. He claims that the majority of networks he comes across are "wide open" to internal abuse. And while few employees are deliberately malicious or fraudulent, he says, organisations must have a clearly stated policy regarding the use of its IT systems in order to deal with dishonest members of staff.

"You can't expect to investigate or prove anything unless you have a policy framework," he says. "You have to have some kind of known-about policy about the use and abuse of IT facilities. Without that, you'll never get to first base in court or at a tribunal." The policy, he adds, must be clear, both to employees obliged to sign up to it, and to the company's lawyers. "There's a case at the moment that hinges on whether it was legal for someone to copy some files," confides Vissilis. "If it was, the whole case falls apart, but the policy document isn't clear."

In contrast, May says the problem of internal abuse is usually one of education. "You can't blame staff for breaching policy or giving out confidential information over the phone if they haven't been made aware of the issues. The best thing you can do is to provide staff with awareness training." One sales person he encountered defended the theft of customer contact lists by other sales executives by saying "everyone does that".

This also holds true for temps and contractors, who must be made to sign up to the company's IT policy if they are to use the system. Vissilis came to the aid of one organisation that had hired a contractor as a database administrator who was abusing the company's IT resources. It subsequently emerged that the contractor was helping a far-right

terrorist group – not a common occurrence, fortunately.

AUDIT TRAIL

But when an abuse does occur, companies must be able to prove what happened and who was responsible. "It's all very well suspecting misuse of company assets, but you need to record exactly what has been done to prove a case," says Stephen Tsirtsonis, technical sales executive at Axial, the UK distributor of a forensics tool NetVCR, which collects and records user activity data for replay at a later date.

Vissilis says that most corporate IT systems come with out-of-the-box logging facilities, but "almost 99% of IT managers turn them off" to conserve processing power and data storage resources. He recalls a client that dismissed an employee for abusing its email system. With the former employee threatening to take the company to an industrial tribunal for unfair dismissal, Vissilis was called in to investigate. However, he discovered that the logging system had been turned off, and he could only narrow down the cause of the email abuse to a group of 15 potential culprits. "All 15 people were tarred with a slight slur on their name. The individual suspected had a strong case for unfair dismissal. The investigation had left the company worse off than before."

Companies must avoid crossing the line of legality, however. Vissilis and May both caution against monitoring individuals without good reason because of the concerns of the Human Rights Act. The Regulation of Investigatory Powers (RIP) Act only allows for the general monitoring of employees' phone calls and use of IT equipment, provided they have been told they will be monitored.

May says the degree of logging is up to the culture of the company. Some companies only log exceptional behaviour, but others monitor everything. The latter end up with large logs that are impossible to read and analyse except with custom tools such as those from data recovery specialist Vogon. But other approaches are emerging. Peter Dorrington, business solutions marketing manager at business intelligence tools company SAS Institute, says that the company's new text mining tool, SAS Text Miner, is capable of analysing logs for patterns that might indicate abuse, but can also spot patterns in other types of documents such as CVs and invoices that might otherwise be missed. "One guy was submitting invoices that individually were not unusual, but together meant he was working a 36-hour day. The accounts department rubber-stamped the individual invoices because there was nothing suspicious about them," says Dorrington.

Cliff May, Integralis: "It's much easier for someone internal to damage systems."

But what about the abuse that is perpetrated by the people most adept at covering their tracks – the IT department? Mark Knowles of Maxima, a fraud investigation agency, says that he is mainly called in over downloaded pornography, and the culprits are mostly to be found in the IT department. "Admins tend to be very helpful. And very good at deleting logs," agrees Vissilis. "You've got to try and second guess what they've done and hope they're lazy or there's something they haven't thought of." Taking regular back-ups of logs, preferably onto read-only media such as CD ROMs that can also be digitally signed, means that even if the logs go missing, they can still be recovered. This can be especially important if a company sets its logs to recycle after a certain period to save space.

ADDRESSING ABUSE

So what should an organisation do if it suspects its IT systems are being used for criminal activity? According to guidance from IT security firm @Stake, it is essential that a record of the computer system be taken as soon as possible. Clues are deleted and distorted during every minute a system is active, making the process of recovering information more difficult for security architects to extract. The International Association of Computer Investigative Specialists lists three essential requirements of a competent forensic examination: "Forensically sterile examination media must be used, the examination must maintain the integrity of the original media, and printouts, copies of data and exhibits resulting from the examination must be properly marked, controlled and transmitted." Tools like Niksun's NetVCR and EnCase from computer forensics specialist Guidance Software take exact copies of a hard drive,

High-tech crime

MODERN technology can not only make new crimes easier, it can create whole new crimes.

• In 1984, a computer programmer at a bank in Kuwait identified a series of five dormant bank accounts (their owners had either forgotten about their existence or had died), opened five accounts of his own and then compiled a program to transfer sums from the dormant accounts into his own, before deleting itself and any trace of his activities. The program did not activate until he left the bank's employment and he was on a plane back to England. In England, he opened accounts with banks and tried to transfer the monies into the new accounts. However, the bank found out about the program and he was arrested before he could withdraw the money.

• An insurance company was faced with a claim for £100,000 for loss of data from a company's central computer. The company claimed a "large industrial magnet" had flattened the computer and that all the data had been lost from the hard drive. Computer forensics subsequently proved that the data on the hard drive was, in fact, intact.

• An accounts firm discovered its software was having problems with dates after 1999, despite having hired contractors to make their systems Y2K compliant. An audit revealed the contractors had not installed any Y2K-compliant updates to the system.

• Employees of various companies have been found running web sites for their own companies from their desktop PCs and one telesales company discovered a sex chat line being run from its offices – it wasn't until it started monitoring network traffic that it found out about it.

• 'Salami' frauds occur when employees skim small amounts from large numbers of accounts in order to bypass internal controls. Before computers, the paperwork involved to collect large sums would have been prohibitive. Now, say specialists in computer forensics, information technology makes salami fraud all too easy.

MOST COMMON ABUSES OF IT SYSTEMS

VIRUSES	32%
PORNOGRAPHY	31%
PRIVATE WORK	12%
FRAUD	7%
HACKING	7%
UNLICENSED SOFTWARE	6%
INVASION OF PRIVACY	3%
THEFT	2%
SABOTAGE	1%

SOURCE: AUDIT COMMISSION

IT facilities most affected by IT abuse

1. Email
2. Desktop systems
3. Web site
4. Administrative information systems
5. Personal records
6. Systems software (for example, database, operating systems)
7. Telephone systems
8. Human resources systems
9. Creditor payments
10. Accounting

Source: Audit Commission

including free and 'slack' space (space partially occupied by files that cannot normally be used by other files).

Getting hold of this evidence can sometimes be more difficult with laptops, says May, but most people under investigation fall for the simple ruse of "the necessary software upgrade", although in more extreme cases, he reports, he has had to fake breakdowns that require the computer to be returned for "repairs".

However, a computer forensics tool in inexperienced hands can be counter-productive. Says May, "The most common thing is for someone in senior management to grab someone from IT [to run an inspection using the tool]. They then change file modification times and overwrite information by installing utilities." The result, he adds, is that vital evidence may be lost completely. There needs to be a well-known procedure for employees to follow in the event of a suspected crime that details what to do and to whom to report the problem. Even trivial matters – such as a Windows screen that previously wasn't there that requires a password (and which could be a program designed to steal the password) – should be reported and logged in case of a potential breach of security.

VARIED SKILLS

Kevin Lack, a partner at Insight Consulting, says the skills required in investigations are extremely varied. "They must have knowledge of systems, programs, monitor-ing tools, interviewing methods and legisl-ation. They have to be able to act as expert witnesses, sustain investigation management skills and even be able to handle the media." So while companies such as Microsoft and Boeing can hire their own in-house forensics teams, the millions of pounds required means that external forensics teams are almost a must for serious crimes. Indeed, if a company discovers child pornography on its systems, the police have to be called in or else the company is aiding and abetting the perpetrator.

With tools such as Vogon, the company's forensics specialist can examine the copy of the computer hard disk and uncover deleted files, secondary accounts, hidden files, encrypted files, files hidden in invisible partitions or alternate file streams, and uncover patterns in disguised files that give away their true natures. If the file is encrypted, it might not be possible to read it, but if the company has forbidden file-encryption in its policy document, the employee can still be dismissed.

However, proving that someone is responsible for the activities on his or her computer is a different matter from proving the computer was used for a crime. Police sergeant Gurpal Virdi was accused by the Metropolitan Police in 1998 of sending racist emails to himself and other officers. While there were forensic blunders in the case that meant the wrong log was checked for evidence of his sending the emails, it was the physical evidence that proved his innocence – he was at another police station when they were sent.

Peter Dorrington, SAS: "Text Miner is capable of analysing logs for patterns that might indicate abuse."

"It's one of the hardest parts of forensics," says May. "You can establish an email was sent from someone's email account, but you can't prove their fingerprints were on the keyboard at the time it was sent. I investigated a case where a machine had been implicated in sending pornography. The desk where it was situated had photographs of its owner's grandchildren on it – 60-year old women with grandchildren rarely distribute child pornography."

May argues that companies need good authentication systems, strong password systems and a clause in the IT policy that makes it an offence for an employee to tell anyone their password. Physical security – in which people are restricted to areas to which they have access and nowhere else – needs to be enforced, even though there is "an English tendency" not to challenge people. He recalls a company where he found a complete stranger had walked in off the street and started using a terminal – without anyone challenging them.

Most cases of internal IT abuse rarely reach trial or even tribunal because of the costs and the difficulty of proving cases. Sometimes the investigation opens a "whole can of worms", according to May, and individuals are implicated that management had not suspected. But without the tools, the policies and the methodology, a company can do little more than grin and bear it.

CONTACT

Article by Rob Buckley
Email: rbuckley@infoconomy.com