IT SECURITY MATTERS

DON'T TRUST YOUR PHOTOCOPIER

Anyone who has ever bought a printer or photocopier for the office knows that it is more than a mere beige box of tricks that prints documents.

Once you've signed up for your new acquisition you're on the hook for a lifetime of invoices for paper, transparencies and toner. That doesn't necessarily benefit the printer manufacturer as you probably buy A4 paper from your favourite stationer and you may choose to buy after-market toner instead of the genuine stuff from HP, Kyocera or whoever. When it comes to accessories such as sheet stackers, staplers and paper trays the manufacturers have got you over a barrel but the real expense comes with internal upgrades such as memory and hard drives.

Taking the HP Colour LaserJet 9500 as an example we see that HP lists a 128MB memory upgrade at a startling £532 or you can upgrade the standard 20GB hard drive to a 40GB unit for £573. No wonder the printer companies are so keen to flog hardware upgrades with those sorts of margins but it turns out that the hard drives in printers and copiers come with the potential for horrendous security problems.

John Juntunen of US company Digital Copier Security (www.copiersecurity.com) is pushing a piece of software called INFOSweep priced at 20 bucks that wipes data from the hard drive of your printer or copier before you dispose of the old unit, presumably because you're buying a new copier.

What harm, you might wonder, could there possibly be in selling off your old copier or simply sending it away for recycling?

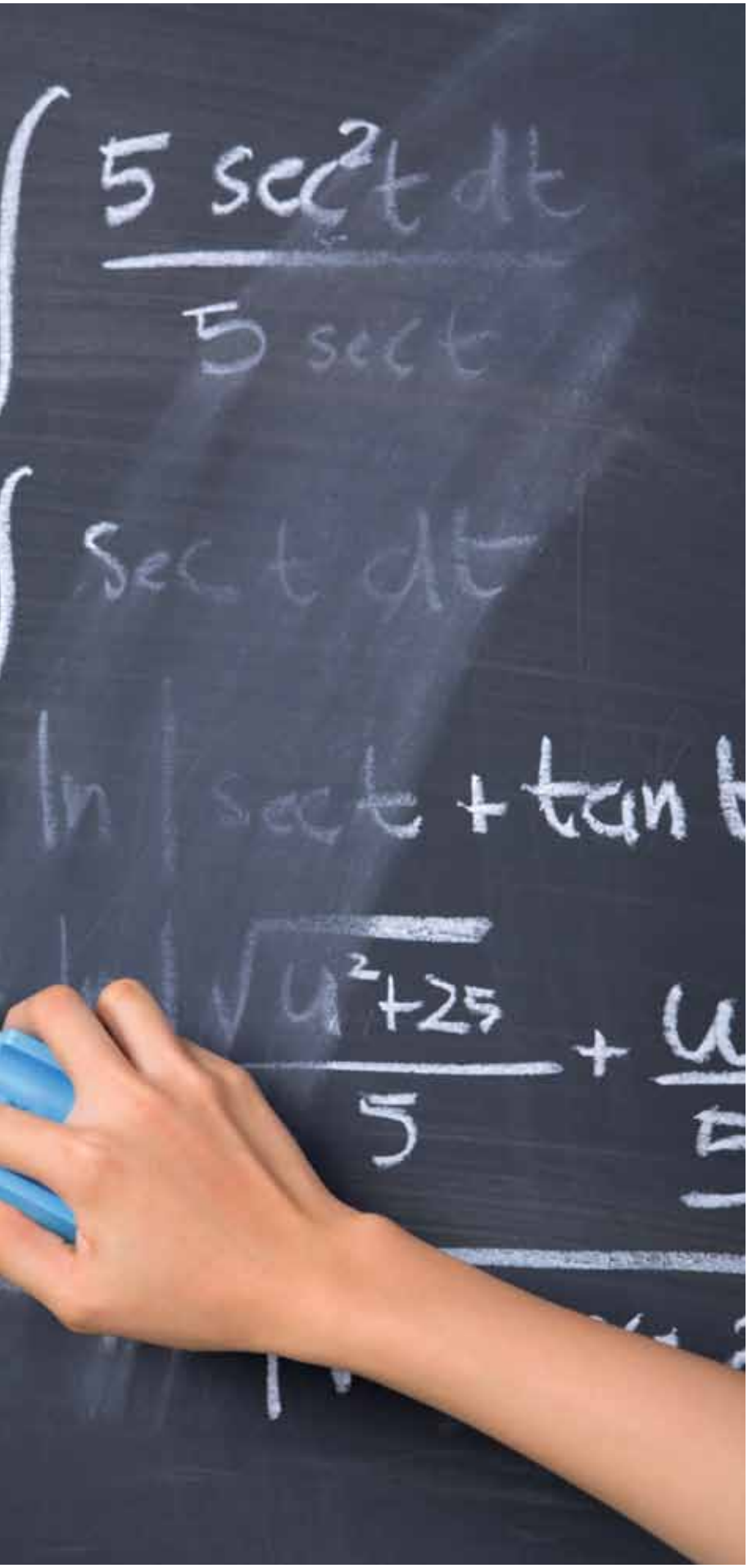
It was reported on CBS News that Juntunen visited a warehouse in New Jersey and picked four used copiers for which he paid US$300 each. Once he got the copiers back to base he removed the hard drives and ran what is described as 'forensic software program that is available for free on the Internet'.

It became apparent that the copiers had previously been owned by the Sex Crimes Division of Buffalo, New York, Police, the Narcotics Unit of the Buffalo Police, a New York construction company and a New York insurance company.

The Sex Crimes copier came complete with the final document that had been copied still on the glass but it was the hard drives that delivered gold including crime reports, lists of wanted criminals, medical records, pages of pay slips and pages of copied cheques.

In short the drives were filled with information that you can be sure the owners would prefer to keep private. It's not hard to argue that the institutions in question have fallen short of their duty of care and may well have breached data protection laws.

'When the time comes to dispose of the old kit you need to remove the hard drive and erase the data or you might as well park your filing cabinets on the street with the drawers left wide open.'



‘It was the hard drives that delivered gold including crime reports, lists of wanted criminals, medical records, pages of pay slips and pages of copied cheques.’

It’s something of a mystery why the printer companies haven’t made more of an effort to pre-empt this problem, although the small matter of hard drives that sell for £500 may be a factor. These days they may well offer an upgrade that encrypts the drive in your new copier, at a price, but that’s no help for your existing hardware.

You’d have thought it would be a simple matter for the companies to add a locked compartment to the copier that contains a USB port that could be used for upgrades. The customer could simply plug in a flash drive for an instant upgrade and when you sell the copier you could pop the drive out and either use it in another copier, securely erase the data or use a coal hammer to utterly destroy the sucker.

In the meantime you’d be strongly advised to view old copiers and printers with the sort of suspicion that you reserve for laptops and mobile phones. When the time comes to dispose of the old kit you need to remove the hard drive and erase the data or you might as well park your filing cabinets on the street with the drawers left wide open.