by Tom Rataj

End of life digital data security

Stop and think for a moment about how much of your personal and business life is digitised and stored on computer hard-drives, USB keys, smart-phones, PDA's, CD's and DVD's.

Depending on what it is, the information will have varying degrees of value to you… and to criminals. Business computer hard-drives, especially in the policing field, may also contain a substantial amount of confidential and restricted information that could jeopardise any number of sensitive investigations or prosecutions, even putting officer's lives at risk if they were to fall into the wrong hands.

We entrust most of our digital data to the lowly computer hard-drive because it has proven to be extremely reliable. Reliability is typically rated in "mean time between failure" (MTBF), expressed in hours. Many manufacturers now advertise a MTBF rating at 500,000 hours (57+ years).

Drive failure

Despite these seemingly lofty ratings, many of us have suffered at least one hard-drive failure at some point during the past 25 years.

Most are the result of internal mechanical components failing or no longer functioning correctly, most often caused by excessive heat due to inadequate air circulation around the drive.

When a hard-drive fails, the data on the storage discs within it is usually perfectly fine, but just very difficult to retrieve.

Rescuing it is big business. Although expensive (thousands of dollars depending on how broken the drive is), it is technically possible and routinely done.

Drive full

Despite the massive capacities of typical desktop and even laptop computer hard-drives, some users do eventually run out of space and upgrade to a larger drive. The retired hard-drive often ends-up in a desk-drawer without much thought about what to do with it and all its precious data.

Life cycle

In the business world, policing included, most laptop and desktop computers are leased for three or four year terms and then replaced with a new machine.

The end of life-cycle computers are usually shipped back to a supplier with the hard-drive intact and loaded with gigabytes (GB's) of readily accessible data.

On your "personal" computer the hard-drive is no doubt packed with GB's of sensitive data, including banking records and other financial files, e-mails, photos, music, videos, documents and spreadsheets.

On business computers, especially those used in policing, there is probably a large amount of highly sensitive and confidential data stored on the hard-drive. Its acquisition, use and storage, decommissioning and destruction is strictly controlled by CPIC and RCMP policy and your agency's data access and storage rules and regulations.

Many sophisticated business class photocopy machines (also often found in the policing environment) feature hard-drives used in the imaging process. These too can often contain years-worth of confidential information and should also be treated in the same manner as a failed or decommissioned computer hard-drive.

Back-up, back-up…

Because hard-drives do fail on occasion, backing-up their contents is also very important.

In a home environment, this is usually accomplished using DVD's or a portable hard-drive. Both the Windows and Apple operating systems ship with back-up software and many DVD burners and portable hard-drives include some type of back-up software.

In the business environment, most computers are routinely backed-up to one or more hard-drives on a network server.

One important consideration that is often overlooked when backing-up a hard-drive is storing the back-up media or device in a different physical location than the original, to safeguard against theft or calamities such as fires, floods or severe storms.

Deleted!

Many computer users erroneously believe that selecting a file and clicking "delete" actually erases the file.

What this simple action really does is tell the computer operating system that the place occupied by the file on the hard-drive is now free to be used. Until new data is written to the actual physical location it occupied, the file can be easily retrieved. If its entire physical location

is over-written by a new file or other data, then a user would need a specialised "un-delete" utility to retrieve it.

Higher-end commercial utilities, including the tools used by forensic accountants, police investigators and presumably CSIS and other spy-type agencies, can actually retrieve files over-written a number of times.

For the home user there are a number of free utilities that effectively delete all the data on a retired hard-drive by overwriting it with random data. Commercial versions of these tools use advanced techniques to completely delete data to top level government specifications.

Digital media destruction

Many people have a paper shredder at home or use a confidential paper shredding service at the office.

There are also digital media shredding services that can shred entire hard-drives in mere seconds, effectively destroying all the data on them. These services should be bonded and insured, meet a number of standards and have valid certifications such as those established by the National Association for Information Destruction (NAID).

For police digital media, the contractor should also be certified by agencies such as the RCMP, CSIS or the Canadian Industrial Security Directorate (CISD).

The continuity of digital media destined for the shredder must also be assured at every step of the way, starting with a secure collection, storage and transportation container or lock-box, through to the transportation and storage of the media prior to the actual destruction process.

Canadian federal standards for digital media destruction are driven by the level of confidentiality of the data, starting with unclassified, protected A, B and C, up to and including secret and top-secret. Each of the three major types of digital media has its own standards.

Magnetic media

For magnetic media (hard-drives, floppy-discs, magnetic tape cartridges of various types, magnetic stripe cards) there are two standards depending on the classification of the data.

Destruction standards start at relatively large 76x76mm pieces for drives and discs down to pieces no larger than 6x6mm. Magnetic tape destruction standards start at pieces no longer than 50mm and end at pieces no longer than 6mm.

Triple overwriting or magnetic degaussing may be recommended by a Threat and Risk Assessment (TRA) prior to being shipped for disintegration or shredding.

Optical media

This includes CD's, DVD's and other discs read by lasers. Destruction standards range from pieces no larger than 12x12mm, down to pieces no larger than 3x3mm. Grinding the disk surface to remove the optical layer and leaving behind only the clear plastic base is also acceptable.

Many better quality consumer grade and most business grade paper-shredders also include an optical media shredding slot that shreds discs beyond the above standards. For small volume shredding these would suffice.

Miniature electronics

This standard includes such items at USB thumb drives, personal digital assistants (including smartphones such as BlackBerrys) and other flash-memory based devices (presumably including the newer solid-state hard-drives).

The destruction level ranges from requiring the reduction of the device into pieces no larger than 12x12mm, down to grinding or pulverising the memory chip in the device.

Resources

The Government of Canada's Communications Security Establishment web site is a good starting point. Check-out www.cse-cst.gc.ca for more information.

The Information and Privacy Commissioner of Ontario, also has some good resources to provide guidance on developing and implementing information security processes. Check-out www.ipc.on.ca for more information.

In southern Ontario Absolute Data Destruction Inc. is a certified handler of digital media. Check out: www.absolutedatadestruction.ca for more information. Outside of southern Ontario, search the Internet for "hard drive shredding Canada" to locate local services.

Tom Rataj is *Blue Line's* Technology columnist and can be reached at technews@blueline.ca.
