

Avoiding catastrophic security leaks in printers and copiers

 By Jacques van Wyk 3 Sep 2015

Carte Blanche, on August 30, highlighted the need to secure documents on copiers, printers and multifunction printers (MFP). These devices contain hard disk drives (HDD) that store data villain can later reproduce.

And they couldn't be more correct.

Securing the information on those devices is a crucial element in the chain to meet regulatory, compliance and general data and information security requirements in the modern, connected age, particularly when handling sensitive data.



hyena reality via [freedigitalphotos](#)

As the segment highlighted, many devices that had reached end-of-lease terms and were then disposed of, still contained their hard drives, unaltered. Nobody had formatted the drives, magnetised them to destroy data, removed them, opened them, nor destroyed the platters they contain that store the actual data. In some cases, data on the drives were encrypted but a skilled person using software downloadable from the internet could retrieve the data and reproduce any of the documents the drives contain - encrypted or not.

The threat

Drives picked up from a local e-waste facility by the Carte Blanche team contained such documents, including sensitive financial information from a church, tender documents, company letterheads and more. Crime syndicates could use the information to access bank accounts to syphon funds, or disgruntled employees to sabotage the organisation (one of the most common types) or by a competitor to disrupt a tender or another nefarious purpose.

Eight solid tips

Carte Blanche posted these [eight tips](#) to its website to counter this threat. They offer sound advice.

Since most of these devices are leased or serviced and maintained by the internal IT department it is important to engage vendor's security services. Any vendor worth their salt will offer them, yet they are not always enforced. People, as with many IT systems, are the weakest link in the chain. With that in mind and considering the potential reputation loss for the vendor involved we have a certified, audited process for any machines that we work on, whether it be to service them or when they reach end of life.

What your vendor should provide

1. Before the vendor removes the device from the customer's premises they should inform the customer of the potential threat, offer to leave the drives onsite, or insist on following the necessary procedure should the drives remain in the device.
2. The necessary procedure is twofold: (a). For devices reaching end-of-life, the drives should be removed, formatted, physically opened, the platters removed and physically destroyed. The same applies to RAM modules and fax boards. (b). For devices under maintenance or service, the drives should not be connected to any networks nor removable data storage media, a format service should be offered and a waiver signed by the customer in the case of refusal.

3. Most importantly, for both procedures, the entire process should be audited for verification and certificates issued for every device.

Four phases of document security on your devices

There are four phases to securing the documents your devices handle, with escalating security threats from phase one to four:

Phase 1

- Restrict unauthorised device access
- Control device output

Phase 2

- Secure network devices
- Secure network print data
- Destroy latent data

Phase 3

- Physically secure data ports
- Encrypt Web communications
- Authenticate users

Phase 4

- Monitor and control resources
- Audit all device activity

ABOUT JACQUES VAN WYK

COO of Ricoh SA
[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>