# Document Security Solution Specialists

Duncan Waugh (Biography)

Founder and CEO of Document Security Solution Specialists (Pty) Ltd. (**DSSS**)

Since 2007, Duncan has proved to clients that Hard Drive (IT) security is not the only area of concern when it comes of the Protection of Personal Information, or any other sensitive information.

As a result of the European Union creating the Data Protection Act in 1995, Duncan has monitored the development of the Protection of Personal Information (Bill) Act from its embryo status to present. Seeing the need to provide an exceptionally unique and necessary service to Government, Health, Commerce and Industrial Sectors alike, he founded and established Document Security Solution Specialists (Pty) Ltd., specialists in completing the cycle of Information Security Management through testing the integrity of physical document security relating to Personal Information and Data, as well as other proprietary and sensitive information

With 36 years' experience in Physical and Information Security as well as Forensic Investigation, including Questioned Document Examination and intelligence gathering, Duncan specialises in the removal and / or recovery and analysis of hardcopy documents, whether it is fragmented, shredded or whole. Upon the reconstruction of hardcopy documents and files, he identifies the type of information normally harvested by criminals, terrorists or intelligence agents, whether it is private, privileged or even secret information. As a result, he identifies the risks pertinent to Organisations, recommends solutions and provides onsite training.

---

The Presentation :

The Title

*Recognising The Paper Peril – The First Step*

**Overview**

Organisations spend billions of Rand each year to protect data, proprietary information and personal information contained in computer hard drives and servers. How many pay any attention to the Management of Information Security relating to hardcopy documents printed by the same banks of computers? Probably without exception, the printed hardcopy documents contain the very information and data Organisations use so many resources to protect whilst contained in a server.

How many even consider the threat of discarded hardcopy documentation?

Excluding hardcopy documents from Information Security Management means that an Organisation's strategy needs to be redefined, because it is certainly not Defence-in-Depth Strategy

**Key Questions**

- We deploy shredders. How effective are they and what guarantee to we have that employees use shredders effectively?

- We operate a paperless business, how can we be at risk?

- We place sensitive hardcopy documents in secure locked boxes for a recycling company to remove, how can we possibly be at risk?

- What is the information contained in hardcopy correspondence used for and by whom?

- How could any of this affect me or my Organisation?

- Now that I have realized there is a very real danger with regard hardcopy documents, how do I identify problems within my Organisation?

- How do I manage potential information leaks through irresponsible storage and disposal of 'waste' paper – hardcopy material?

- If I do not include any tangible procedures in my Information Security Management Systems to monitor hardcopy documents, what could the results be?