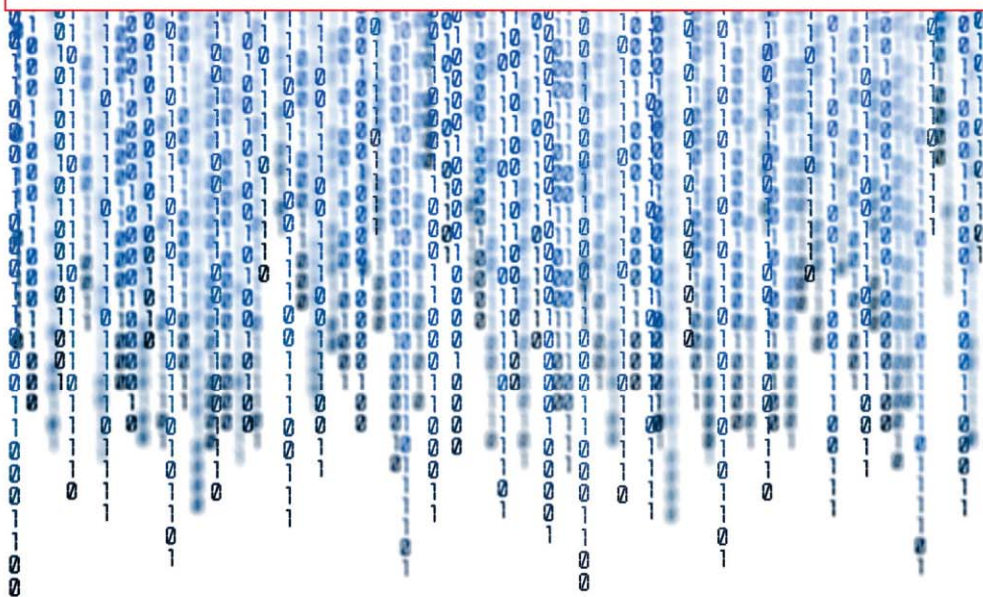


you can
Canon

Connecting Technology

Information Assurance



INFORMATION ASSURANCE

We Speak Image

Introduction

Security is undoubtedly an area of much focus throughout both the public and private sectors. The risks of breaches to security and Information Assurance (IA) policies range from a reduction of operational/business continuity and costly inefficiencies to damage to an organisation's reputation and reduced stakeholder and public confidence. In extreme cases, a breach, or lack, of policies can even have serious legal implications.

As with any involved issues, it comprises areas of great complexity as well as several Quick Wins which are easy for most organisations to adopt.

Security is now much greater than simply physical access restrictions

Along with the priority of security moving up most corporate agendas, there has been a change to the actual definition of what security is. The issue is now much greater than simple physical access restrictions. Security has been expanded in scope to include difficult-to-manage areas of data and information, processes and ownership. This new scope has been re-defined under the banner Information Assurance (IA) which involves the management, integrity and availability of information – not only its restriction.

What are the Main Issues?

Within the parameters of document and data workflows, there are numerous elements where an IA issue may require consideration, especially with the advancement of office technology. The benefits of more sophisticated technological can mean considerable cost and process wins to most organisations, but ownership of the information is required to optimise IA compliance.

- It's not commonly known that multifunctional printers (MFPs) have hard drives. The result is that the type of security processes applied to PCs/Servers are often not considered relevant..
- MFPs store data – both volatile and non-volatile
- Many users/IT departments are not aware that the MFP is also an entry point to a network, otherwise known as a “Network Node”
- MFPs/Printer are also key data exit points (although it is difficult to extract sizeable amounts of data in hard copy compared to digitally). Most offices enable all users to print anything without checks or controls.
- Standard IT security Policies often don't consider the above – this is often made worse by limited knowledge of the technical capabilities of print technology and how to mitigate risk

It's not commonly known that multifunctional printers (MFPs) have hard drives. The result is that the type of security processes applied to PCs/Servers are often not considered relevant

Despite these issues, there are numerous advantages to adopting a multifunctional printer-based approach to document workflow. The technology can enable an audit trail for documents and user activity auditing. This level of assurance is not available in traditional un-managed print environments.

Legislation and Standards

Information assurance (IA) is the practice of managing information-related risks. More specifically, IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation.

Common Criteria: This is a recognised security standard set by international security agencies providing recognised levels of IA.

The 2008 Hannigan Data Handling Review called for enhanced accountability for secure data. Secure MFDs and an auditable print workflow have the ability to enhance accountability around the document workflow.

The Data Protection Act, this requires organisations to comply with a number of criteria to protect business and personal data. There is a legal provision to create data ownership and where relevant, end-of-life disposal.

Next Steps

What does this brief intro into the world of IA mean for an organisation? It is probable that there is a significant benefit to the vast majority of organisations in adopting an increasingly robust process and ownership model for the data life cycle.

With this in mind there are a few entry-level recommendations for the use of multifunctional printers to assure current data more robustly.

1. Whilst multifunctional printers are in use, ensure data encryption options are enabled on hard drives and that there is a provision for data overwrite functionality for “in use” data.
2. Deploy device-release print to add a level of assurance over who prints what and when. If backed up with a Document Accounting capability this can enhance the IA of the document/data workflow.
3. When multifunctional devices come to end of life a process to ensure data disposal is advisable. As with PCs/flash sticks, ensure a policy for disk disposal such as deleting data which may potentially still be available or destroying the disk for environments deemed sensitive/secure.
4. Ensure an overall level of ownership for Information Assurance similar to Health and Safety where an overall Champion such as CIO/CEO assumes and assures pan-organisation compliance with data policies. This remit will need to stretch to all employees being trained and tasked with a level of IA awareness and compliance.

Further Questions

If the issues outlined in this document have raised further questions which you wish to discuss, please contact:

Neil Palmer – Information Assurance & Coherence Manager
e-mail: neil_palmer@cuk.canon.co.uk
Mobile: 07970 214 112
www.canon.co.uk/publicsector

INFORMATION ASSURANCE

ENVIRONMENT

COST MANAGEMENT

you can
Canon

Canon (UK) Ltd
Woodhatch
Reigate
Surrey RH2 8BF
T: 08000 353535
F: 01737 220 022
www.canon.co.uk

Canon Ireland
Arena Road, Sandyford
Industrial Estate
Dublin 18, Ireland
T: 00 353 1 205 2400
F: 00 353 1 295 8141
www.canon.ie

