Information Security White Paper

Document Security

Protecting business information

Contents

Introduction

Every day organisations process thousands of documents, in all types of formats, and every day they are in danger of being lost, stolen or compromised. They need protection.

Sharp defines Document Security as security related to information captured from paper documents through the scanning process or digital documents stored in business repositories, for example, Microsoft Office files, emails, etc.

Sharp Document Security covers:

- Document related business processes
- Document storage
  (physical paper documents and electronic archives)
- Document lifecycle
  (Capture > Store > Manage > Preserve > Deliver > Integrate)

This White Paper outlines the challenges every business faces in relation to document security. The main points discussed are:

The Background

Examines the complexity of Document Security. From identifying all office documents and information in the most common business processes through distinguishing paper (physical) and electronic (digital) types of documents, to a description of the document lifecycle process.

The Problem

Describes the challenges that IT managers, end users and management in business organisations can face from a Document Security perspective, especially when capturing, storing and accessing business-sensitive documents and information. *The focus areas are:*

- Unstructured data
- Manual tasks related to office documents
- Overall Document Security.

The Recommendations

Outlines how Sharp Optimised Solutions, services and best practices can help build a secure document environment to avoid document security-related threats that could lead to data breach or process disruptions.
This section also explains how Sharp can help you solve complex business problems in the areas of:

- Understanding the importance and role of document processes
- Optimising paper-based archives and electronic file-based repositories
- Identifying all the steps needed for optimising the document lifecycle or creating your own Document Security Policy and best practices.

The Conclusion

Provides a summary of the topic, and focuses on the following:

- The key business challenges related to documents in the business
- The main recommendations based on Sharp's expertise and Sharp Optimised Products
- The next steps required for building a consistent Document Security Policy
- Connecting Document Security with other aspects of security in the office, including Network Security and Output Security.

Background

Today the speed at which we work and the volume of data we create and consume is increasing at an exponential rate.

> Industry analyst IDC predicts that worldwide data creation will grow to an enormous 163 zettabytes (ZB) by 2025[1].

That's ten times the amount of data produced in 2017.

Every day, businesses create contracts, invoices, proposals and many other documents in numerous formats, all of which are critical to their operation.

Contracts, for example, define the trading relationship between the organisation and their clients, while invoices deliver revenue to the business when paid. Managing, preserving and making this information available to the right people in the organisation is key to a business' success.

> 90% of all data today was created in the last two years – that's 2.5 quintillion bytes of data a day.[2]

The volume, complexity and diversity of information a business creates and consumes leads to challenges in management and control. To overcome this situation a business must understand and map document types - how they are used, how they interact with business processes, how they are stored, managed, distributed and preserved.

Most of these challenges are directly connected to the following three issues:

Unstructured data

Unstructured data is information that either does not have a pre-defined data model or is not organised in a pre-defined manner. Often transactional documents such as emails or office documents are stored by users in folder structures they create with no standardised naming convention or descriptive metadata.

For this reason, it is very difficult to get a unified view making the following questions difficult to answer:

- How are documents stored, managed and controlled?
- How easily can the documents be found, audited and distributed?
- How are access rights and file permissions applied?

Manual repetitive tasks

Manual, repetitive tasks exist in virtually every business, whether it is processing invoices, handling expenses or managing HR documents. Technology can help automate these processes improving efficiency, accuracy and traceability at the same time as improving security.

Understanding the document lifecycle in your business

Every document or document type will follow its own lifecycle from capture through to disposition. Understanding, mapping and optimising the document lifecycles for different document types is key to ensuring that the correct security measures are applied for regulatory compliance, while also providing the degree of flexibility required for efficient working.

These are the key areas that every business should consider when defining and implementing a Document Security Policy for the organisation.

Problem

Modern businesses process a lot of information, but often don’t have true visibility of how it is produced, stored and accessed, which leads to potential security flaws.

Most organisations embrace digital content creation and storage, however, documents are often stored in two formats electronic (digital) and paper (hard copy):

- Paper files/records
  Hard copy documents in paper or other formats present a considerable security risk, since it is often difficult to prove their provenance or show a clear audit trail, leading to a lack of traceability. In addition, consideration of physical security is often overlooked where, for example, sensitive documents in process are mis-filed, lost or stored in unsecure locations.
- Electronic files/records
  Electronic records stored in distributed and sometimes isolated storage systems present their own security challenges often due to the sheer volume and potential number of storage systems/locations. Understanding the lifecycle of documents is the only way to establish company-wide processes and security policies.

Maintaining Document Security

The definition of Document Security (or lack of) is very wide and should be considered from the perspective of the document lifecycle, especially in relation to: data breaches, unstructured data, unsecured files, human failure, unauthorised access to the storage, etc.

The document lifecycle consists of six main stages – Capture, Store, Manage, Preserve, Deliver and Integrate:

Stage 1: Capture
Capture is the process stage that describes the ‘on-boarding’ of information, whether that is scanning of hard-copy documents, monitoring a ‘watched’ email ‘box’ or creating and saving documents from an application:

- Scanning is the most common way of transferring hard copy content to electronic formats. But while scanning is convenient it can lead to security and legal admissibility challenges. Without controls, the process is not traceable, so documents may fail the evidential weight and legal admissibility test.
- Indexing is the method used to describe documents using meta-tags or full content (text). Indexing facilitates fast file searching and data discovery - tools that are especially useful for reviewing content in relation to security of compliance.
- Routing is the process used to send captured documents to the correct storage location. Without document routing it is possible that documents can be inadvertently stored in incorrect or even insecure locations.

Stage 2: Store
Secure storage can be paper-based or an electronic file system, but many companies overlook the storage type, location and security required:

- Paper-based storage systems are still very common, but often lack the required security controls. In addition, it is very difficult to show any audit information related to paper documents
- Electronic based storage is often implemented with the expectation that it is a better way. However, without appropriate design and management it creates challenges, including, for example, how such systems should be protected in the business network, how to setup access rights, and how to monitor or restrict usage.

Stage 3: Manage
Document management covers permissions, version tracking and audit trails:

- Permissions are used to manage users’ access rights to documents, so they are key in maintaining a secure document environment. While permissions are often easy to understand, without the right systems they can be difficult to introduce and manage. To implement permissions effectively the business must first understand how users’ activity relates to the information they must access and the processes they are involved in.
- Version tracking ensures that users are working with the latest documents while preserving, where necessary, previous document versions. This is especially useful in strategic or legal situations where the provenance of the document can be proven by reviewing previous document iterations. Version tracking is key to maintaining a secure and legally admissible digital document archive.
- An audit trail stores records of every activity and transaction applied to a document, including, for example, who created, modified, viewed or re-versioned it. Audit trails provide the ability to prove activity relating to all documents stored and are key to maintaining security, particularly in the event of a data breach.

Stage 4: Preserve

Preserving documents and information is another key aspect of ensuring a secure document environment. However, documents that are stored in traditional or electronic repositories require constant maintenance, as the available space is limited. So, the following procedures are crucial:

Document retention

Some documents should be kept (by law) for a certain number of years. The challenges in doing so include:

- Maintaining a record to ensure only documents beyond the retention period are removed
- Ensuring that all versions of the documents under the retention policy are accounted for
- Deciding how documents should be managed either centrally or locally.

Document disposal

Businesses need to set policies to securely dispose of all paper information, electronic files and electronic libraries once they are out of date or the retention period has expired:

- Physical document shredding is the traditional way of dealing with paperwork following one of the DIN Shredding Security levels. It can be a costly and time consuming.
- Electronic shredding means secure and verifiable erasure of electronic documents from hard drives, DVDs, floppy discs, etc.

Stage 5: Deliver

This stage defines the ways that an electronic document can be shared with other users or business partners. In particular:

- Document sharing is frequently done by using shared folders or drives but, if not managed correctly, this can lead to the files being found, accessed and used by unauthorised users or user groups
- Accessing documents through mobile devices can also be part of the deliver stage, which brings much more complex issues regarding securing the access.

Stage 6: Integrate

Integration is the process used to exchange information with other line of business applications, such as, an accounting or ERP system.

For integration to be successful, correctness and completeness of all the preceding stages are critical to provide consistent and accurate data. Problems in any of the points raised will have a direct impact on the business process.

Recommendations

Sharp can deliver a number of solutions and applications that can help organisations create a necessary Data Security Policy.

The matter of Document Security is very complex, but defining the document lifecycle structure makes it clearer and easier to understand, and then change or enhance:

- Improving processes or defining Document Security from scratch can be quite difficult and time consuming, especially when mapping processes and capturing all of the relevant information on processes and business roles. Sharp Professional Services use both our experience in the document solutions industry and sophisticated tools for document/information discovery and workflow mapping.
- Sharp uses a step-by-step process to help businesses understand their current document lifecycle and related challenges, then uses these to develop the processes and procedures to address the two main goals of optimising Document Security:
  - *To bring structure to unstructured data*
  - *To accelerate and streamline repetitive tasks.*

Getting started quickly and safely

- Sharp helps customers create robust security policies and document environments. Based on a combination of Sharp MFPs for capture and our Optimised Software Portfolio for document storage and management, our solutions give customers the peace of mind that their document infrastructure is secure and traceable.
- As a start, this may just be changes in process for paper-heavy departments (HR, Finance or Legal), then later extending the process and procedures to other areas of the business, with planned steps.

Simplifying document capture and storage

- To ensure scanning is secure, Sharp strongly advises that customers only scan to secure, internal repositories and selected email groups or users, all of which can be configured by IT administrators on Sharp MFPs. This is especially important when considering GDPR compliance.
- Where more sophisticated capabilities are required, perhaps to support legal admissibility, these can be provided using Sharp's Optimised portfolio of products. Sharp offers a variety of solutions that accelerate processes in small, medium and large organisations and enable direct integration to business applications.
- Sharp Optimised Solutions give the option to index all captured documents:
  - *Add metadata directly from the MFP*
  - *Add metadata at the application interface prior to storage and processing.*
- Sharp Optimised Solutions include routing options, to ensure that all users scan and capture in the same, structured way and then direct documents to the correct, relevant locations and trusted applications.

User Roles & Permissions

When building a Document Security Policy, user permissions and roles are important to preserving confidentiality and control.

- Sharp advises using one central document management system with 'roles' linked to employee's business needs. For example:
  - *Only Board level members can access all business documents*
  - *Only HR can access staff records*
  - *Project managers can access project related documents*
  - *Sales representatives can access sales-related files like brochures, forms, etc.*
- Permissions are defined on a role or group basis to control what users can do with documents – create, view, change, delete documents – or a subset, for example, so the user can view documents without any other rights.
- Version tracking is essential. The Sharp Optimised Solutions allow you to check which version of the document you are working on, and review or recover older versions of the document.
- Concurrent working is supported by document management, such that if one staff member is editing a document other staff will be limited to a read only view.
- To ensure security compliance goals are being met, IT administrators can use a sophisticated audit trail tool (audit logging trail), which records every document activity including when a document was changed, who changed the document and how long a specific user was working on it.

Keep the right information for the right time

- Design a document retention policy based on the type of the document and the departments that process the information.
- Document disposal is the end point of the document retention policy. Depending on the type of repository in use, there are options for removing all data from your systems:
  - *For paper documents Sharp advises using a professional shredding service that has at least a DIN 5 rating*
  - *For electronic data Sharp advises using a professional electronic data wiping service*
  - *For data stored on HDDs (using on-premise document management and internal repositories) Sharp advises a two-step process – data wiping and then physical destruction to ensure access to the hard drives is not possible.*

Seamless information access and sharing

Every Document Security Policy introduced to the business should describe how users/employees can access documents and how they can share the data with others.

Sharp Optimised Solutions offer several methods to deliver documents through document management platforms:

- The first option is to share a link to the file by email to the addressee with a link expiry timing. Details of the share activity are logged, and the link can be terminated on demand, or by a pre-set timeout period.
- The second option is to share folders within the system with registered users from the same organisation. You can decide and set he rights of the recipients – 'read', 'read write', 'read write delete' – to work on the documents in the folder. These rights and rules can be also established when designing the overall document management system rules and Document Security Policy.
- Most functionality of the system can also be made available to mobile workers, either on Android or iOS. Sharp recommends that businesses consider the advantages of secure mobile working.

Getting optimum value out of your data

Sharp has developed a number of integrations, so that the data captured through Sharp MFPs, or hot folders or connected applications, can integrate with business systems, like Sage, QuickBooks, SharePoint and more.

Examples of departmental areas that Sharp has focused on are:

Optimised Workflow Software for Accounts Payable

The solution uses Optical Character Recognition (OCR) to extract the data from captured invoices, and automates the validation and approval processes. It enables an "accounts payable" department to operate with increased productivity, improved accuracy and seamless efficiency.

Learn more.

Optimised Workflow Software for Digital Mailrooms

The solution captures incoming paper and digital mail and routes electronically to the correct staff or representative in the event of an 'Out of Office' notification. It helps businesses quickly and efficiently sort and distribute high volumes of post, maximising the productivity of staff.

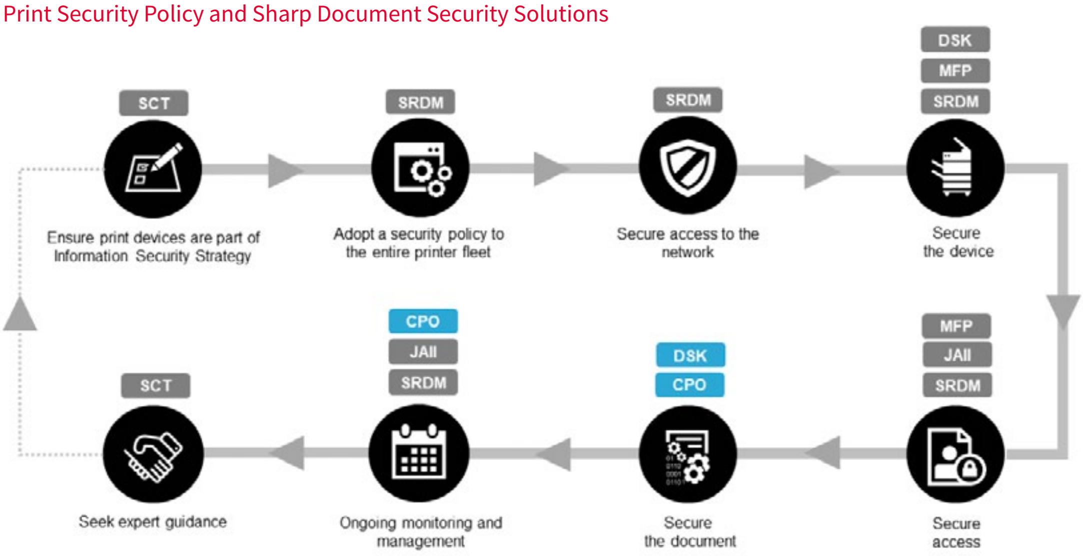
Learn more.

Optimised Workflow Software for Human Resources

This solution introduces a highly secure and managed repository for confidential staff documentation. Businesses can streamline the processing of HR documents, control the access to documents, and achieve compliance with Data Protection and privacy regulations.

Learn more.

Building Print Security Policy and Sharp Document Security Solutions


SCT
Ensure print devices are part of Information Security Strategy
SRDM
Adopt a security policy to the entire printer fleet
SRDM
Secure access to the network
DSK
MFP
SRDM
Secure the device
MFP
JAII
SRDM
Secure access
DSK
CPO
Secure the document
CPO
JAII
SRDM
Ongoing monitoring and management
SCT
Seek expert guidance

SCT – Sharp Consulting Team, SRDM – Sharp Remote Device Manager, DSK – Data Security Kit, MFP – Multifunction Printer, JAII – Job Accounting II, CPO – Cloud Portal Office

Conclusion

No one can afford to ignore information safety, especially when it involves documents. They are the intellectual wealth of every organisation and their loss can be devastating.

Document Security is one of the most important aspects of security in every business. Unfortunately, building a Document Security Policy can be a time consuming and complex process. This is where Sharp can help.

Sharp has years of experience in the Document Solutions industry that has enabled us to develop a comprehensive approach to data security in business – from Network Security, Output Security through to Document Security.

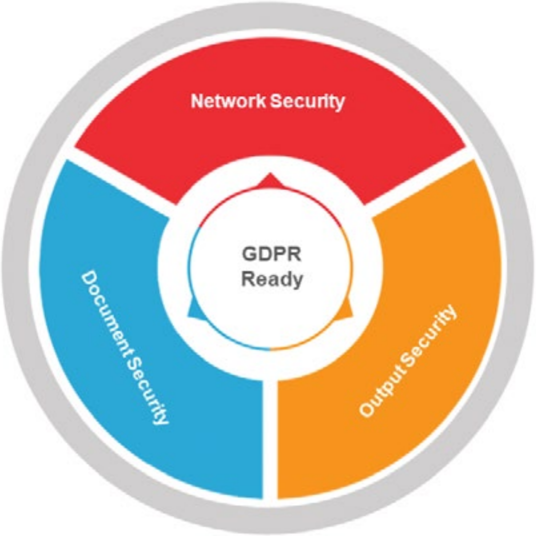
We aim to help our customers build robust and compliant security in their document related business processes through our expertise and globally recognised leadership in Office Security matters.

Using our proven approach to Document Security we help businesses build unique and bespoke systems and processes for each of the document lifecycle steps (Capture, Store, Manage, Preserve, Deliver and Integrate) and, in doing so, help those organisations comply with the latest security regulations, like the EU's General Data Protection Regulations (GDPR).

Sharp Optimised Solutions are designed to deliver maximum functionality and security, together with a quick return on investment.

Key verticals for Sharp are the Government, Education, Legal, Financial, Healthcare, Hospitality and Corporate sectors, however, we can deliver bespoke and robust solutions to help every type of business.

Sharp Security Framework



To avoid potential vulnerabilities in other areas of your organisation, we can help you introduce further security measures from the Sharp portfolio, so that you can deliver 360-degree security protection for every aspect of your business:

- Document Security
- Network Security
- Output Security
- GDPR compliance

You can find more information on the above topics in our White Paper library or in the Information Security section on our website:

www.sharp.co.uk/cps/rde/xchg/gb/hs.xsl/-/html/information-security.htm

Alternatively contact your Sharp Solutions Consultant.

References

1. Data Age 2025. *IDC. March 2017*

2. Data Never Sleeps 5.0. *DOMO, 2018*