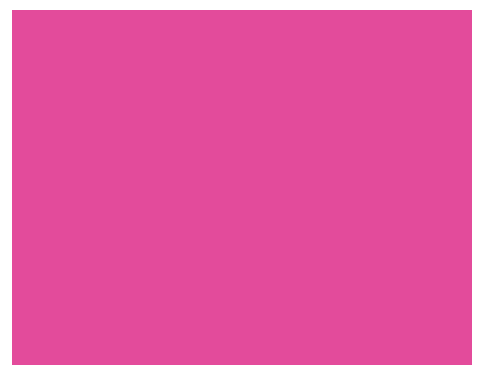# FUJI XEROX

Reputation Management

Vital consideration for every business

What is your print security and content sharing strategy?

We live in a world today that is more connected, more informed and empowered. The scenario of a Chief Executive Officer waking up to see his company mentioned on the front page news because unfavourable content was shared by an employee is more likely to happen today than a few years ago.

Before reaching out to brand reputation management tools and social media monitoring applications, it may be worth evaluating a more fundamental question – can I improve my print security and content sharing strategy in my organization? Is my current risk and information management strategy up to date,

and can allow me to effectively navigate the complexities of reputation management.

"How do I ensure my information management policies reflect the needs of our changing workforce, empower my employees to perform at their best, not hinder decision-making or customer service excellence? At the same time, I need sufficient safeguard measures to mitigate my cyber security risks, corporate espionage/leaks, and other sources of risks that compromise data security and privacy?"

– Chief Technology Officer

"In the war for talent, reputation management impacts employee engagement rating and my credibility with people I'm looking to attract. How can I ensure our information management strategy is progressive, promote greater levels of engagement and is a positive talking point in the market?"

– Human Resources Manager

Business requirements	Business impact
Information management	Reduce risk in information leakage correlates with lost business opportunity and adverse impact on corporate image You can improve that by • controlling who has access to print, scan or copy on Multi-function Devices to mitigate information leakage or theft of confidential information. • generating Multi-function Device usage trail to enhance information traceability and audit trail for content sharing. • controlling access and sharing of content on cloud storage services.
Digital rights management	Protect company assets from illegal plagiarism by, • controlling the use of, modification, and distribution of copyright materials such as software and multimedia content • Install systems within devices that can help you enforce these policies.

How Fuji Xerox can help you handle your Reputation Management Scenarios

Before

There are many gaps in information, content and document security in the workplace. There is little consistency in how digital data is managed.

01
Documents exist in shared folders and there are no restrictions on who can access, share or print them.

02
There is little or no control over how key digital information (contract, IP or legal documentation) is secured from prying eyes.

03
Any employee can potentially steal your data and share it with competitors, vendors or the media.

04
There is very limited support for mobile use and no security policies on how company data is used on such devices.

Solutions:

ApeosWare Management Suite, ApeosWare Image Log Management, Card Authentication, DocuShare, DocuWorks, Digital Rights Management

After

A simple document security strategy can help you mitigate information leaks and unauthorized content sharing.

01
With document rights management capabilities and access to secured cloud storage services, you can share content safely and securely with external parties.

02
Users are required to authenticate their identity in order to use the MFD to scan, print or upload content to cloud services. A single button activates digital rights management, enabling specific policies (e.g. print rights, number of views, time to self-destruct) to be applied to documents.

03
All user access to data is logged and audit trails can be created at any time.

04
Everyone can work securely from their mobile devices, access and print documents from the cloud.

05
From the comfort of your desk you can create a folder to manage scanned files and add digital files inside, just as you would when handling paper documents. You can also add a pass code, a Digital Signature or Annotate on the digital documents.

ApeosWare Management Suite and **ApeosWare Image Log Management** allow you to maintain ongoing records of your document movements (copy, scan, fax and print) and who has accessed it from the Multi-function Device.

Card Authentication allows users to seek access permission in order to use Multi-function Device functions

With **DocuShare**, you can set access policy for documents maintained in this enterprise management platform. You do not need to worry about content being viewed or accessed by unauthorized users.

Digital Rights Management allows you to set relevant print rights, how many times documents can be viewed, when it will self-destruct.

With **DocuWorks**, you can scan documents and send them out in a secured file format. Documents in different formats can be put together in a folder, and you can add a digital signature to them to meet added security requirements.

Talk to our Sales representative today to learn more.

For more information, please visit www.fujixerox.com.sg/smartworkgateway

For more information or detailed product specification,
please call or visit us at

Fuji Xerox Singapore

80 Anson Road #01-01 Fuji Xerox Towers Singapore 079907
Tel. +65-6766-8888
http://www.fujixerox.com.sg/

FUJI xerox