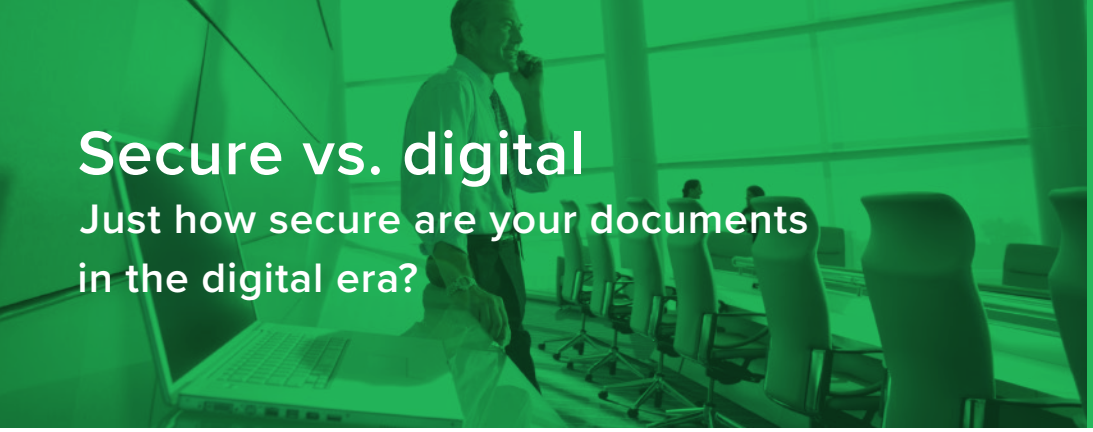

Secure vs. digital

Just how secure are your documents in the digital era?

Similar to a music file, each digital document in a company can be reproduced infinitely without any loss in quality. While this often makes our daily work more flexible, it also open the door to misuse – unless clear rules are established.

The acronym cc (for carbon copy) in an e-mail header dates back to the time when copies were made by slipping carbon paper between the sheets, regardless of whether a document was written by hand or created on a typewriter. Anyone who's tried out this method of duplicating letters will have discovered that there are physical limits to the possible number of copies: by the fourth copy the text suffers serious legibility issues. E-mails and messenger messages have virtually eliminated these limitations, which is not always helpful in everyday working life. Particularly in companies with large team structures or strict hierarchies, the feeling is that everybody should be included in the information loop and certainly never ignored, even unintentionally. As a result, messages with countless recipients in "carbon copy" abound. This is perfectly okay for seeking out donations for a colleague's birthday or for sharing the date of an important trade fair.

A mouse click is not without risk

However, since many of us have to deal with sensitive documents all the time – contracts, prototype sketches, orders, personnel files and the like – we should be aware that these sometimes critical attachments must not be made accessible to a broad number of people. Unfortunately, we are only human, and it can easily happen that a birthday mail is accidentally sent out with a wrong attachment. The result is that even the receptionist now knows about the new prototype. These serious security breaches can be avoided by following certain protocols. For anyone who relies on technological solutions, the logical next step is to implement a document management system.

KYOCERA
Document Solutions

Sensitizing people to security issues

We all enjoy the many benefits of the digital age, such as being able to quickly retrieve, edit and distribute digital documents with ease. While these advantages have become indispensable, it is extremely important to create a deep awareness in all employees about the sensitive nature of data and the need for observing clear guidelines. Wherever capital funds “data” is at stake, training sessions and educational work are mandatory. At the very least, all employees should at least know there is a Federal Data Protection Act that every company is required to observe*. Legal data protection requirements exist to protect sensitive internal business processes as well as the personal data of employees, customers and other people involved.

* This is only an exemplary case in Germany.

Implementing a document management system

Aside from enlightened employees and secure data capture, a document management system (DMS) can also prevent the “biggest conceivable accident” from happening, namely that a classified developmental sketch is made public in a birthday mail. The advantages of such a solution are not limited to storing all digital documents in a space-saving, secure and legal way, compliant with the latest retention policies. You can clearly define which user may access, edit or share a certain document, and that is valid for all data in an electronic archive.

A DMS solution provides a central digital archive which allows you to retrieve any required document regardless of whether it is cause- or content-related. This will invariably reduce the number of digital “carbon copies” – a similar challenge to the one which confronted businesses in the era of carbon paper.

See how KYOCERA can help you establish a secure and managed document environment at our enterprise content management (ECM)-related website.