Protect Your Business Information:
Prevent Document Deterioration, Misuse and Loss with EDM

By Laurel Sanders, Optical Image Technology

Digital capture gives *you* control over your content.

S ecurity concerns are in the news a lot lately. The government has issued public alerts against terrorist activity. Military experts are debating how to maximize armed forces' safety amid intensified conflict in Afghanistan. Medical experts are producing vaccine to combat Swine Flu. Each issue focuses on the need to ensure public safety. Yet most businesses – including agencies that rely on timely, accurate information to make decisions about public safety – overlook a serious risk that jeopardizes their effectiveness and ability to survive. The threat? Inadequate document security.

Businesses need secure access to accurate information to make smart decisions.   Usually information is scattered:

- on paper (subject to deterioration, misfiling, security breaches, and loss);
- trapped in the minds of executives, managers and workers (subject to unintentional alteration and selective memory); and
- stored in electronic documents and software applications (subject to inconsistent rules, conflicting policies, and difficult to lock down).

A recent 2009 AIIM report entitled *Electronic Records Management – Still Playing Catch-up with Paper* shows 60% of managers surveyed couldn't be confident their records hadn't been altered, deleted, or inappropriately accessed if they were challenged. More than 70% had no provisions for long-term electronic record archival; 31% had twenty or more content repositories that could be usefully linked (and presumably weren't, complicating access and security). Many respondents described their electronic records as unmanaged; most lacked email management policies. It doesn't take an expert to uncover a foul brew of document security concerns. Ignoring document security invites trouble.

Set clear policies
Document security has two sides: human and technological. Management has the onerous job of weighing rules and regulations against operational needs and determining acceptable risks versus those that jeopardize their business objectives. Identifying unacceptable risk is a precursor to creating governance policy.

Communicate policies frequently – in writing
Rules are futile unless they're communicated – frequently, understandably, and in writing. Understanding what constitutes risk, acceptable behavior, and the penalties for disobedience dramatically reduces employee blunders. Convey your rules and reasoning clearly. Document your communications. You'll reduce company risk by demonstrating *intent* to comply.

Well-laid plans, smart hiring decisions, and regular communications minimize risk, but they don't guarantee document security. Where 100% document control is hindered by human limitations, web-based electronic document management (EDM) excels – governing, observing, and tracking file use, 24/7.

DOCO
D o c F i n i t y
Optical Image Technology, Inc.

Imaging, BPM/workflow, and
Document Management Software

Emulate policies electronically

Everyone hears about planned security breaches. Yet typically, compromised document security is *un*intentional:

- People view sensitive information while searching for unrelated information.
- Employees inadvertently destroy original files without noticing copies or imported documents are faulty or illegible.
- New employees don't know the rules and handle documents improperly.
- Temporarily removed or inappropriately stored documents can't be located on demand for audits, subpoenas, or processing.
- Workers delete documents deemed worthless, learning afterward that retention rules changed or they were mistaken.

EDM ensures security from the moment of capture, preserving file integrity throughout the business lifecycle and providing a central repository for stored information.

> Employee logic varies for document classification and search. EDM enables standardization, making filing consistent and search 100% successful.

Readability and integrity are verified upon capture. Digital storage eliminates deterioration, misfiling, or loss. Files are readable, properly stored, and secure. Customizable security determines who can retrieve, view, edit, annotate, manage, move, or delete files. Administrators can set rules for data use and walk away, knowing employees can access whatever they need.

Remove temptation and filing mistakes

Companies are increasingly subject to strict regulations governing information use. EDM enforces your governance policies, letting you:

- Restrict file access by creating pre-defined searches to retrieve files staff need.
- Restrict document viewing to specific personnel by job role and document type.
- Associate individual editing and annotation rights to pre-specified users and file types.
- Ensure only authorized persons can delete batches, files, and/or pages of documents.

Assure consistent indexing

Employee logic varies for document classification and search. EDM enables standardization, making filing consistent and search 100% successful.

- Assign documents to batches during scanning or importing.
- Index documents by document type, customer ID number, and other unique identifiers.

- Associate related documents for a comprehensive view of information.
- Validate the integrity and accuracy of scanned and imported files through automated validation; request alerts when documents require intervention.

Digital capture gives *you* control over your content.

Prevent document alteration

Document alteration poses huge security risks, especially in the face of litigation and audits. ECM allays fears of inappropriately altered documents. You can:

- Restrict document annotation and alteration rights to pre-designated persons.
- Ensure file alteration and editing rights reflect current policies.
- Store business-critical emails as unalterable documents.

Avert inappropriate file deletion

Missing and lost documents typically comprise 7.5% to 11% of all document requests, with workers spending anywhere from 20-50% of their time looking for information. MIA documents cost time and money to recreate; if they're needed for an audit, subpoena, or industry mandate and not found, penalties can accrue.

EDM ensures documents aren't deleted until they're *scheduled* to be migrated or destroyed. By limiting user rights, you ensure against accidental and intentional purging. Automated retention assures document migration, purging, and deletion follow your

> EDM ensures documents aren't deleted until they're scheduled to be migrated or destroyed. By limiting user rights, you ensure against accidental and intentional purging.

rules. Regulatory changes? No problem: EDM grasps new instructions immediately, adhering to governance directives.

Adjust rules as hierarchies change

Between a quarter and a third of employees change jobs or positions annually. Promoted employees suddenly need access to additional information. Demoted workers lose rights to access particular documents. Some are fired or leave, creating concerns they may take information with them, and new problems arise as knowledge must be transferred to new hires.

EDM tackles these issues with ease:

- Users and feature rights are pre-designated electronically, making appropriate files accessible immediately to new employees.

- Administrators make documents instantly *in*accessible to departing employees by deleting user rights and features, eliminating the risk of inappropriate file use.
- Rules and rights are easily reconfigured, ensuring new employees can access repositories and files they need without the risk of stumbling on sensitive information or overlooking policies for document access and use.

Lock down email

Email management eludes many managers. Critical communications about customers, partners, third-party vendors, staff, products plans, licensing information and more often are trapped in email Inboxes, inadequately archived and difficult to find.

By managing business email within EDM, you can:

- Index and archive critical emails as documents of record.
- Restrict access to email content, while disclosing contents to authorized persons.
- Regulate printing, migration, and deletion of stored emails to specific users.

Avoid disaster

The topic of avoiding business disasters drew attention this year when the Association of Corporate Travel Executives (ACTE) recommended that companies limit how many executives can travel simultaneously on the same corporate or commercial plane. Experts recognized that a single calamity involving the loss of multiple top-tier executives constituted unacceptable risk, as it could destroy a company and result in considerable job loss. The same is true with the loss of your business-critical documents.

Document preservation is the left hand to the right hand of document security. Careful planning, quality EDM, and appropriate professional services ensure you have:

- Effective backups and fault-tolerant, redundant systems that ensure you stay connected to your information.
- A disaster recovery plan that outlines the hierarchy of document importance to ensure business continuity and accelerate document recovery.
- Uninterrupted access to your business-critical information if a disaster prevents staff from working onsite.
- Physical data recovery in case a real disaster strikes or your system is shut down.

Forge ahead

If your company makes the headlines, don't let it be because of a security breach or shutdown. Creating a document management strategy and investing in EDM means your past, present, and future documents will be in the *right* hands, whenever and wherever they're needed. By leaving the arduous task of document management to EDM, you'll have more time to focus on taking your business to the next level. Good luck!

> EDM ensures security from the moment of capture, preserving file integrity throughout the business lifecycle and providing a central repository for stored information.

DOC∞
D o c F i n i t y

Optical Image Technology offers an integrated suite of imaging, document management, and workflow software, including document archiving, lifecycle management, electronic forms, and email management products. To learn more about our products and services visit our website at www.docfinity.com, email info@docfinity.com, or call us at 800-678-3241.