Access denied – navigating the digital information security maze

Out there, in the corridors of power, the compactuses of restriction and assorted business systems, there's a war going on. It's the 'War of Access'.

By **Kevin Dwyer** and **Michelle Linton**

In the 'War of Access', the fight is over who can, who should and who will see 'my' records. The two armies slogging it out in this cold war are the people of the business defending their right to individually and inconsistently determine who will see their records and the stewards of information, records management.

Prevarication rules as organisations avoid the proactive conversations necessary to make the hard decisions to develop a mature organisation-wide approach to accessing records – hard decisions that not everyone will like. The factions continue to reactively squabble with each other over the rules of operation and how to apply them and very little progress is made towards a better world.

When managing only paper records, business easily wins the fight. The Records and Information Management (RIM) team receive paper records when the business deems them to be important information needing protection. If the business doesn't want RIM or others to see the information then they simply don't tell them about it. It is squirrelled away in locked filing cabinets, personal drives or restricted access Windows folders. And of course only emailed to people that are trusted!

The business has a myopic view that their information is incredibly secure. They see some exceptions of course, such as when their 'trusted' friend shares the email – innocently or otherwise, or those few other people who know their password use it or when the building burns down/is flooded. They see the likelihood of these incidents as so rare that it is not worth the complications of thinking about the security decisions to protect the organisation from the consequences.

The 'that won't happen to me' mentality fails to note that these 'rare' incidents have happened in almost every known organisation with disastrous consequences to reputation, finances and operations.

RIM has ploughed on, despite the resistance and the apparent desire of the business to fall on its own sword, to fight to protect their organisation's physical information assets. Then along came digital records in an electronic document and records management system (EDRMS). What a bonus! Now it's possible to register all records as they are created, apply appropriate security from the outset, control and audit who viewed, edited, shared, etc. the record, and reduce the risk of information loss for the organisation. RIM is now in a position to truly meet their responsibilities.

However, many businesses continue to thwart the best efforts of RIM through a somewhat tedious and erroneous list of excuses for not adopting organisation-wide access and security practices:

- *"I can never find records once they are in the EDRMS."*
- *"All it does is stop my team from accessing records they created."*
- *"Why should the RIM team have access to my sensitive records?"*
- *"People should come to me and ask my permission to see my records each time they want access so it might as well be in my shared drive."*

story snapshot

When a project is run to increase EDRMS adoption rates, there are inevitable fears about access to records.

Reluctance to embrace the EDRMS with good recordkeeping practices leads to higher risk to the organisation.

Information assets are managed by an information security approach that seeks to protect confidentiality, integrity and availability.

Configuring the EDRMS to meet an organisation's security policies and procedures is often tricky.

When a RIM team runs a project aimed at increasing EDRMS adoption rates amongst users they inevitably run up against fears about access to records either from the viewpoint that "Everyone will be able to see my files", to the other extreme of "I'll never find them again".

To win the battle, RIM needs the business to have faith that the records necessary to do their job can be accessed easily. At the same time, they need to have confidence that truly sensitive information is not viewable by unauthorised people. These are the cornerstones in gaining the trust of managers and users to move to or increase the use of digital recordkeeping.

It's not simple to create this environment of trust. The business has its own ideas of what security and access means and how to apply it. It's challenging to create the security protocols and environment that can be correctly interpreted and willingly applied by the business across multiple recordkeeping systems that keep records in digital, paper and other physical formats.

A lack of knowledge of information security as a topic and the role of recordkeeping and the use of EDRMS functionality helps create and perpetuate myths and stories that reduce that faith considerably and perpetuate the reactive war. Sadly, the result of this reluctance to embrace the EDRMS with good recordkeeping practices is higher risks to the organisation and reduced productivity.

UNBUNDLING INFORMATION SECURITY

It is important when trying to navigate the word of digital information security as applied by an EDRMS to understand the context in which it sits.

The starting point of managing information security is for an organisation to understand what its information assets are.

An information asset is information that has value to the organisation. An information asset may not be a record. A record, being evidence of a business decision, is most likely to be, however, an information asset. In most organisations, information assets are managed by an information security approach that seeks to protect:

- confidentiality, by ensuring that information is only accessed by authorised individuals
- integrity, by ensuring the accuracy and completeness of information
- availability, by ensuring access to information, systems, networks and applications.

A range of approaches including physical security (locks, codes etc.), password protection, intrusion detection and prevention, security classification labelling, encryption, secure shredding and plain simple security awareness protect information assets as part of an information security management system (ISMS).

Recordkeeping practices utilising the functionality of an EDRMS have a large part to play in supporting an ISMS. The EDRMS also creates an auditable security trail throughout the life of the record enabling breaches of security to be managed at their source. Also, in the event of a disaster, there is immediate availability to digital records, increasing customer confidence and reducing loss of business.

SECURITY & ACCESS IN AN EDRMS

Digital information assets deemed to be records and stored in an EDRMS generally have their access described by three attributes: security classification, caveats and access control.

Security classifications

Security classifications may apply to records (documents and folders). The security classifications in the EDRMS should mirror those of the information security policy. The classifications used depend on which standard the organisation wishes to follow. An example is the Australian Government Security Classification (Table 1).

SECURITY CLASSIFICATION	TO BE USED WHEN
UNCLASSIFIED	Information is released within the organisation on the basis of 'need to know' but is not restricted. Information is not released outside the organisation without the permission of the owner of the information.
UNCLASSIFIED with Dissemination Limiting Markers Eg: For Official Use Only (FOUO) Sensitive: Personal Sensitive: Legal	Information can only be released to organisations and individuals with a demonstrated need to know and information is to be stored and processed away from public access.
PROTECTED	Used when the compromise of the information could cause damage to the Australian Government, commercial entities or members of the public – eg, tender documents.
CONFIDENTIAL	Used when the compromise of the information it relates to must be considered as possibly causing damage to national security – eg, damage diplomatic relations.
SECRET	Used when the compromise of information could cause serious damage to national security, the Australian Government, nationally important economic and commercial interests, or threaten life – eg, raise international tension.
TOP SECRET	Used when the compromise of information could cause exceptionally grave damage to national security – eg, lead directly to widespread loss of life.

Table 1: Australian Government Security Classification

The first level of classification is UNCLASSIFIED, which should be the default. UNCLASSIFIED can be strengthened by use of a dissemination limiting marker (DLM). Their purpose is to restrict release of information to a group of people for a purpose. For example, a record classified UNCLASSIFIED: Sensitive: Legal is likely to be restricted to people in the legal department.

The levels of classification impose increasing restrictions on their storage, distribution, copying and destruction.

Most organisations will have well over 95 per cent of their records classified as UNCLASSIFIED or PROTECTED (or equivalent eg, in-confidence).

Caveats

A caveat is a warning that the information has special requirements in addition to those indicated by the security classification. It is generally used to limit specific types of records to specific roles across an organisation, such as HR records types to HR roles. When it is used those people who need to know about its use need be involved and educated. Others in the organisation do not need to know about the use of caveats.

Access control

Access controls are the most specific level of security applied to records in an EDRMS. Access control is an individual

⇛

security control and is applied to individual records. Access controls restrict access across a range of properties such as: View Document, View Metadata, Update Document, Update Record Metadata, Modify Record Access,

Access controls when thought through well, combined with security classifications usually provide sufficient security control through an EDRMS.

EDRMS OBJECT CONFIGURATION

Configuring the EDRMS to meet an organisation's security policies and procedures is often tricky. At a minimum there are three objects to be configured: record types, profiles/ locations and classifications.

The goal is to determine how to apply a combination of security attributes to each of the objects in a complementary manner. When an EDRMS was a new digital records system the simplistic approach was to provide each business group with their own record type and security configuration. It was not unusual (and is still prevalent) to see 25 folder types, one for each branch, and 25 document types as well. Specialist record types were in addition to this. Not only was this a nightmare for RIM to maintain, it supported information silos rather than information access, and users complained.

As EDRMS configuration has matured RIM has become aware of complex combinations of object configuration that minimise maintenance and promote improved sharing of information. Using the previous example, a folder record type with default full access to the owner of the record, and view-only access to all other groups, combined with inherited security for document record types, reduces 50 records types to two.

NAVIGATING THE CHALLENGES

Security and access and object configuration is not new. It exists in physical records management. The difference is it's enforced in an EDRMS. That can make it difficult for even the best recordkeepers in an organisation to adapt to the change.

Imagine this scenario. You're an executive assistant in Branch 1. The director of Branch 2 requests a record that is classified as confidential to Branch 1. You know this record has been discussed with the director and they have had input into it. In a paper-based world it was easy to decide the information could be shared with this person and to take a copy and send it around. Rightly or wrongly it happened. In a Windows folder world it is printed and provided. In an EDRMS, any action on that record is audited and the breach of security recorded. The answer to the director must be no. The executive assistant is not happy, the director is not happy, and the EDRMS is seen as restrictive rather than upholding the policy of the organisation.

To avoid this unhappy circumstance being the norm in an organisation, there are several simple things which need addressing.

Overuse of security and access controls

The most common issue plaguing the application of security policy to an EDRMS is the over-classification of records and the over-use of access controls.

People who have come from an environment of personally designed file structures on a shared drive have a sense of 'ownership' of information that goes well beyond any requirements of information security. They are loath to share their information with colleagues in their section let alone the whole organisation. The consequence of extending this approach to an EDRMS is to make records unavailable to staff who have a need to share the information.

The result is frustration and unproductive work by the RIM unit and the end-users as permission is sought and gained to open up access to the records. Over-classification results in unnecessary, administrative arrangements that remain in force for the life of the record. The volume of security classified information becomes too large for an organisation to protect adequately. Over-classification brings security classification and associated security procedures into disrepute. This often leads to security classifications being devalued or ignored by organisation employees.

The default security level should be UNCLASSIFIED. The default access control for all records should preferably be the whole organisation. The vast majority of records should be viewable by anyone in the organisation. This is rarely the case. Higher classifications should be used sparingly and only when the record meets the requirement of the classification. Most organisations, for example, will have very few, if any, CONFIDENTIAL records as defined in the Australian Government Classification system.

Policy & procedure

Security is not a popular topic in most organisations. Spend time and effort to make people aware of the policy for applying additional security and the need to abide by the policy and to follow the procedures. Ensure emphasis is given to the procedure for applying for permission for others to have access if necessary.

Continuing education

Make sure people are aware of how security works and what is happening when they apply it. Telling people how to apply security is insufficient. Educate people in the difficulties that result when incorrect security and access options are applied. Have people experience the difficulty in finding a record if view metadata access has been denied, or a caveat is applied.

Be proactive about managing the situation, rather than reactively adjusting access record by record as requests come in. And expect that education is ongoing. Managing the security of information is a priority and the majority of organisations are many years from achieving full EDRMS security maturity.

ABOUT THE AUTHORS

Michelle Linton, Managing Director, Linked Training

Michelle is a Learning & Development professional with 24 years' experience in the planning, design and delivery of training programs. Michelle has developed and delivered innovative, outcome focused EDRMS training for over 30 government and private organisations since 2005. Michelle's pragmatic approach to learning strategies leading to application adoption has been enthusiastically welcomed by the industry, and she is a regular speaker at RIM events and contributor to industry magazines. Linked Training is the training partner in the REX project which was awarded the J.Eddis Linton Award for Excellence – Most outstanding group in 2010.

✉ She can be contacted at Michelle@LinkedTraining.com.au

Kevin Dwyer, Director, Change Factory

Kevin is a Change Management professional with more than 30 years' experience in the planning, design and delivery of change management programs. Since 2001, and the establishment of Change Factory, he has been involved in many Change Management projects ranging from re-engineering of customs processes to reduce risk to creating and revising performance management systems to improve customer service outcomes at five-star resorts. His first EDRMS project was as the Change Management partner for the REX project which was awarded the J.Eddis Linton Award for Excellence – Most outstanding group in 2010.

✉ He can be contacted at Kevin.Dwyer@changefactory.com.au

Wants versus needs

Individuals within the business will provide RIM with a description of what they 'want' in security configuration, which is often overly cautious for the majority of records. RIM must discover the business goal, which will inform the actual 'need'. This is frequently not what was asked for, so demonstration is then required to provide all stakeholders with confidence in the solution.

RIM sense and sensibility

Sense: the ability to think or reason soundly. Sensibility: an acute perception of, or responsiveness toward something.

Sometimes RIM are their own worst enemy by taking a conservative view of security themselves and being very fixed in their approach to applying the security policy to the EDRMS. Take the situation where a manager had been acting up for six months and has written a record that was the responsibility of the higher position. The following year, now seated in the lower position, his manager asks him to update the record. After fruitlessly searching for it, he contacts RIM and is informed access is restricted to the higher level position and above. After explaining the situation and requesting access the answer is a resounding NO.

Technically the RIM staff member was correct, but the person wasn't even provided with the protocol for having the access adjusted. There will always be valid exceptions to a rule, and RIM staff need to be educated on how to manage them and keep people onside.

The reverse situation has been seen also, where the business pleaded for a single unclassified folder type to facilitate cross-functional sharing and enable the executive team to access information. The change required, in both approach and restructuring, was outside the comfort zone of the records unit, and was stubbornly blocked. The business, in return, was equally stubborn in refusing to use the EDRMS. ❖