Strategic value and drivers behind organizational adoption of enterprise DRM: The korean case

Morin, Jean-Henry; Hovav, Anat

How to cite

MORIN, Jean-Henry, HOVAV, Anat. Strategic value and drivers behind organizational adoption of enterprise DRM: The korean case. In: Journal of service science research, 2012, vol. 4, n° 1, p. 143–168. doi: 10.1007/s12927-012-0006-1

This publication URL: https://archive-ouverte.unige.ch/unige:29495

Publication DOI: 10.1007/s12927-012-0006-1

Journal of Service Science Research (2012) 4:143-168
DOI 10.1007/s12927-012-0006-1

Strategic Value and Drivers Behind Organizational Adoption of Enterprise DRM: The Korean Case

Jean-Henry Morin, Anat Hovav

Received: 13 March 2012 / Accepted: 8 June 2012 / Published: 30 June, 2012

ABSTRACT

In the context of now prevalent Extended Virtual Enterprises and our information and knowledge based economies, Enterprise DRM (EDRM) has become an important technical means to address many security issues ranging from simple persistent content protection to more complex dynamic governed usage pattern monitoring. Information is a strategic resource requiring prudent management. Therefore, a better understanding of the strategic value and major drivers behind organizational adoption of EDRM is needed. This paper presents a case study carried out with three large Korean companies. While our initial assumptions led us to hypothesize that compliance management and regulatory frameworks would rank the highest among the drivers for organizational adoption of EDRM, our study found that Knowledge Management (KM) appears to be a leading driver. We also identified Inter-Organizational structure as an increasingly prevalent factor in the adoption of EDRM.

KEYWORDS

Enterprise DRM, Information Security, Adoption of Technology, Extended Virtual Organization, Case Study.

Jean-Henry Morin
Faculty of Economic and Social Sciences, HEC Genve, University of Geneva, Switzerland
e-mail: Jean-Henry.Morin@unige.ch
Anat Hovav, PhD (✉)
Department of MIS Korea University Business School
E-mail: anatzh@korea.ac.kr

1. INTRODUCTION

E As companies continue to progress towards a networked and globalized economy with business processes spanning organizational boundaries, they are increasingly exposing their corporate information assets to prying eyes and potential external and internal misuse of those assets. Corporate scandals and the need for regulatory compliance have fueled a growing interest in operational risk management in the context of what is now known as GRC (Governance, Risk and Compliance) (Tarantino 2008). It is in this context that Enterprise Digital Rights Management (EDRM) emerged as a technical means to address many of the current and future security requirements beyond the traditional access control and perimeter based security solutions (for a discussion regarding the limitations and challenges of traditional identity management techniques see Hovav and Berger 2009).

EDRM refers to the use of Digital Rights Management (DRM) technology in the Enterprise sector. DRM technology is often used to manage digital assets and define the rules governing their use in a persistently protected way. For detailed introduction and description, see Morin and Pawlak (2007).

While traditional adoption of technology literature stresses the operational, economic or strategic benefits of the adopted technology, investments in Information Security (InfoSec) are driven by risk reduction (Gordon and Loeb 2002). Assessing security return on investment (ROIS) is a hard and somewhat speculative task. Similarly, it is difficult to build a clear business case for the adoption of InfoSec technology since it is unclear that such technology could provide economic gain, competitive advantage, or operational cost reduction. Yet, the number of EDRM projects currently being considered and deployed is increasing. Therefore, in this study we attempt to examine some of the major drivers behind organizational adoption of EDRM and describe their potential strategic value. Such a study would provide organizations with general guideline for analyzing the adoption of EDRM and indicate its strategic value to senior security and information officers.

We present and discuss our initial assumptions in section 2. Section 3 describes the methodology of the study. In section 4, we present and discuss the results and future direction. Section 5 introduces the EDRM Maturity Matrix as an assessment and planning tool for EDRM readiness.

2. BACKGROUND ASSUMPTIONS

Adoption of technology literature mostly focuses on the economics of adopting a new technology such as cost, return on investments, financial risk, and network externalities (Fichman and Kemerer 1993). Rogers (1983) discusses the characteristics of the technology and its relative advantage to an organization. Sambamurthy (2000) highlights the value of information technology in supporting strategic initiatives related to knowledge management and knowledge sharing. While the current MIS literature is filled with articles examining the adoption of various technologies, there are relatively few studies that examine the adoption of InfoSec technologies. This is because InfoSec technologies are rarely considered strategic tools, their economic value is hard to measure, they often increase operational costs, and some technologies are removed from the users and may have little impact on work performance. One technology that had been absent from the InfoSec literature is EDRM.

Initially fueled by the media and entertainment sector, DRM technologies were positioned as a possible way to manage content access and its persistent protection requirements. Although entertainment based DRM is highly controversial (Morin 2009), the same underlying technology showed applicability in the corporate sector (e.g. Windows Rights Management Services provided by companies such as Microsoft[1] and LiquideMachine[2]). As corporate information became a strategic asset, its' persistent protection moved from the basement (technical) to the boardroom (strategic). That is, as information security and other information assets scandals (e.g., 2008 financial crisis) became salient, the need to manage digital assets gained the awareness of executives and board members. In addition, as corporate boundaries became fuzzy (e.g., virtual organizations, ad-hoc partnerships, cloud computing) traditional corporate perimeter based security frameworks are insufficient. The third potential adoption driver stems from the growing importance and potential impact of corporate, legal and regulatory compliance.

2.1 Business Value of EDRM

Morin and Pawlak (2007) propose two drivers for the adoption of EDRM, persistent

[1] http://www.microsoft.com/rms.

[2] LiquideMachine was bought by Checkpoint in 2010. http://www.checkpoint.com/.

content protection and corporate compliance requirements. Their study is based predominantly on Western legal and regulatory environment (i.e., Sarbanes Oxley in the U.S. and Basel II in Europe). Thus, our initial assumption led us to suppose that compliance and content management would be key factors behind organizational adoption of EDRM in the Asian context.

Given that Korean organizations have increasingly been relying on information and knowledge to advance their economies, knowledge has become a valuable organizational and even a strategic asset (e.g., strategic planning, trade secrets, embargoed information.) For example, Samsung is one of the leading companies in R&D expenditures in the world. In 2007, Samsung spent $6,536 Millions, the 9th largest expenditure globally (Jaruzelski and Dehoff 2008). Therefore, knowledge management, as a superset of content management, appears as a likely potential driver for organizational adoption of EDRM in Korea.

In addition, considering the increasing need for loosely coupled, ad hoc, and dynamic cooperation among a range of business partners such as joint ventures, short-term consulting, sourcing, and partnerships, there is a growing need for inter-organizational cooperation requiring instrumenting and orchestrating business processes spanning several legally independent organizational structures. Therefore, we propose that inter-organizational structure is a third driver for the implantation of EDRM in Korea. The traditional corporate perimeter-based frameworks do not operate well in virtual environments. For example, Access Control Lists (ACL), are limited to organizational boundaries. Once the content leaves these boundaries (e.g., consultants, partnership, and outsourcing), it cannot be protected, controlled, and managed by the originating organizational unit. Consider the following scenario, a bid is prepared by company A and is posted on a shared server to enable access to several partnering companies and potential vendors. An employee from a partnering company PA downloads the bid to a personal computer and modifies it (intentionally or unintentionally) before sending it to a subsidiary PS. The contract received by PS is different from the original contract posted by A. PS's reply to the bid does not match the original request resulting in potential future rents (loss of a potential contract, sending erroneous supplies, legal action). Once the bid was uploaded to the shared server, company A lost control of the document and the ability to protect the integrity of the information posted.

Consequently, our initial set of assumptions regarding the major drivers behind organizational adoption of EDRM in Korea is the following:

- Compliance with regulations (external) and policies (internal)
- Knowledge Management and Knowledge workers
- Inter-organizational systems processes and structure

Based on Morin and Pawlak (2007), we assume that compliance would rank highest among the three drivers. The next sections describe each proposed driver in more details.

2.2 Legal, Policy and Regulatory Compliance

Compliance with recent regulations require organizations to maintain copies of all electronic records, documents, and communication (including e-mails, video conferencing logs and instant messaging) for long periods (e.g., 10 years for accounting data). As a result, companies need to manage their digital content in an accountable and sustainable way. If a company is asked to provide certain audit trails, they should be able to do so in a timely manner, for a reasonable cost and with little disruption to their daily operation. Regulations such as the K-SOX (Korean version of Sarbanes-Oxley enacted in 2004) also require companies to maintain information such as where the document was created, who saw it, and who modified it. Such requirements often stem from Operational Risk Management guidelines and traditionally fall under the responsibility of internal controls.

Traditional approaches are often based on simple repository structure (e.g., NFS[3], NTFS[4]). The record attributes used by these structures are relatively crude, and can be easily modified by various hacking tools.. These structures do not support today's digital forensics' requirements. Recent Korean privacy laws[5] also require that organizations limit accessibility to private information to authorized persons on a "must see" basis. Passwords and ACL protection only safeguard information at the first point of contact. Traditional security systems focus on perimeter based security. That is they are applicable only within the boundaries of

[3] NFS (Network File System) refers to a protocol developed by Sun Microsystems. NFS allows clients to access files located on remote servers.

[4] NTFS (New Technology File System) refers to Microsoft's proprietary file system.

[5] Such as privacy and data protection laws regarding financial information, credit card transactions and medical records.

the originating organization. However, once the information is copied or transmitted, the initial protection is no longer in effect. To ensure compliance, organizations need to extend the protection of privacy and control beyond organizational perimeters and beyond the initial point of contact-throughout the entire information life-cycle (i.e., from creation to archival, including all the intermediary steps, some of which are often outside the company's perimeter and legal domain). EDRM enables the originator of the asset to define persistent controls and permissions that span domains and remain for the life of the content whether in motion, at rest or in use. Thus, a read-only document cannot be copied or modified regardless of where it resides at any point in time.

Korea, like many countries, has enacted laws governing the quality and trustworthiness of financial data provided to shareholder and the public (e.g., K-SOX). Senior executives are now responsible and liable, and would face criminal charges in case of fraud. Similarly, Korean laws require the safeguard of private medical records, credit card transactions and other personal financial data. In addition, Korean laws require the protection of classified technology. This is especially applicable to companies in the hi-tech, electronics and communications industries. According to the laws, both managers and individuals can be held liable and face monetary penalties and/or jail time if information is leaked. In addition, managers need to convey these laws to employees to ensure compliance. Therefore, we propose the following:

> *Proposition 1: compliance with regulatory requirements will drive the adoption of EDRM. Specifically, organizations operating in an increased legal compliance environment are more likely to adopt EDRM.*

2.3 Knowledge Management

Recent trends, such as managing knowledge life-cycle[6]and the empowerment of the knowledge worker, could potentially compromise traditional privacy policies. Knowledge Management (KM) is about sharing as much knowledge as possible (Davenport and Prusak

[6] Capturing, maintaining (tagging, removing, adding, archiving), and disseminating knowledge.

1998), whereas Information Protection (IP) is about protecting information and providing it on a need-to-know basis. Thus, the two are conflicting organizational goals that need to be balanced.

Empowering employees requires them to have access to organizational data and information at various levels. However, it also enables disgruntled and ex-employees to inflict damage to the organization by divulging information to unauthorized sources. In addition, employees may unintentionally share information, give away their passwords, or leave their computers unprotected. This enables hackers to access sensitive data (D'Arcy and Hovav 2007). Although training, education, awareness and policies help mitigate some of these issues (D'Arcy and Hovav 2009) organizations need to have additional layers of control in case information is leaked intentionally or accidentally. While traditional access controls limit accessibility to information and can be considered as inhibitors to knowledge sharing, EDRM is about managed-accessibility to content and should thus be seen as an enabler to knowledge dissemination (Morin 2008). Thus, EDRM-based Content Management Systems exhibit the property of persistent protection. The fact that access to EDRM-based KMS is always managed allows much more open sharing of information while still maintaining the required level of protection, control and monitoring. Therefore, we propose the following:

Proposition 2: Knowledge work will drive the adoption of EDRM. Specifically organizations with increase knowledge-base processes are more likely to adopt EDRM.

2.4 Inter-Organizational Systems Processes and Structure

Traditional organizational structure where the boundaries are determined by the "formal" configuration of what is *in* and what is *out* of the organization is disappearing. Outsourcing, contracting, partnering, integrated supply-chain, and CRM create fuzzy organizational boundaries. The traditional access control approaches (e.g., ACL) to rights management, which depends on perimeter-based boundaries, are unlikely to work well in organizations with fuzzy boundaries. For example, consultants are a typical example of personnel called to complete missions on an ad-hoc basis. While under contract, they have legitimate access to information assets. Often when leaving the corporate perimeter, they extract some assets onto removable devices, email, etc. for legitimate reasons (i.e., to complete their work in their home office). Such content remains outside the corporate perimeter without any form of protection. Similarly, content posted on a corporate extranet (see example above) can no longer be protected by using perimeter-based controls and is thus susceptible to illegal modifications and leakage. Applying EDRM-based security policies to persistently protected content enables the management of this content through rules governing its usage, wherever it resides and at all times. Therefore, organizations with advanced and flexible structure will be more likely to adopt EDRM, while organizations with traditional structure and boundaries are less likely to need the features afforded by EDRM. Therefore, we propose the following:

> *Proposition 3: Inter-organizational structure will drive the adoption of EDRM. Specifically organizations with increased fuzzy boundaries are more likely to adopt EDRM.*

3. METHODOLOGY

3.1 The Sample

Yin (1994) suggests that exploratory studies that try to answer questions as to “how” or “why” something is done should use case methodology. Eisenhardt (1989) states that case studies should be used when little is known about a phenomenon. Although adoption research is not new, examining the strategic adoption of EDRM by organizations is new. This is especially true since most regard DRM as a way to limit access to multimedia content in the context of music, movies and other forms of entertainment. The use of DRM in the context of organizational policy and content management is relatively new, and therefore this warrants the type of rich analysis case research can provide. For this study, we have selected a multiple case design with a single unit of analysis for each case (also called “type 3” case study methodology (Yin 1994)). This design can provide more compelling evidence by supplying multiple data points by which to test our propositions.

We selected three large South Korean conglomerates (see Table 1). This choice was motivated by two factors: (1) a large portion of the Korean economy is driven by these conglomerates and therefore they represent large companies in Korea, and (2) large organizations are more likely to have given a thorough thought to an enterprise-wide DRM project. Yet, while the above rationale justifies the use of these particular three conglomerates, the three companies is a convenience sample since they were referred to us by an EDRM vendor, rather than selected randomly. All three are Korean conglomerates (i.e., *chaebols*, referring to the Korean form of large business groups or trusts) and are comparable in their overall business structure. Although conglomerates span many overlapping sectors such as Food, Bio, Entertainment, Electronics, Chemicals, Financials, Infrastructure, Construction, Retail, etc., we differentiate them for the sake of this study based on their brand name and products. Table 1 lists the companies we studied.

Table 1. Companies Used for the Study

Company	Domain	Interviewees	# of employees	Comments
A	Food, bio, pharmaceutical	CIO and CPO (in charge of Information security)	4,500	Division within a Chaebol
B	Retail, hotels, food	Division CEO, development director, EDRM project managers	Not Available	A division of B, in charge of all IT projects, and operates as a cost center. The division also bids on external projects.
C	Electronics	Director	260,000	A division of C, in charge of all IT projects, and operates as a cost center. The division also bids on external projects.

3.2 The Interviews

Within each company, one or more senior managers were selected as interview subjects (see Table 1 for details). These managers are directly responsible for information security and EDRM implementation decisions and therefore reasonably represent both managerial and technical perspectives regarding the relevant EDRM project in their respective organization. In cases where more than one manager was interviewed, they were interviewed as a group. Upon agreement to participate in the study, a face-to-face interview was conducted. The interviews followed a scripted set of open-ended questions (see appendix A for an example).

Follow-up questions were asked when clarifications were needed. The script ensured that we followed a similar protocol and asked a similar set of questions in each interview. Yet, the script was adapted to each company's specific characteristics and enabled us to explore additional aspects when necessary. The set of questions were developed based on our propositions and derived from the literature. The questions were phrased in such a way as to be "neutral" so that the interviewee would not be led to answer in a particular way. The first part of the script included a general set of demographic related questions allowing us to categorize the respondent(s) role and function, the industry, and the general IT context of the company. The second part surveyed the actual EDRM project within the company. The third part specifically focused on the drivers (i.e., the three propositions introduced in the previous section) asking the respondents to prioritize them and to answer specific questions within each of the categories (i.e., legal and regulatory compliance, KM and IOS). Finally, after the introduction of a tool described in section 5, the respondents were asked to position themselves in one of the four quadrants of a maturity matrix, at present and in three to five years.

The interviews of roughly two hours each were conducted primarily in English by both authors. An English-Korean interpreter who is also versed in the domain (i.e. EDRM) was present at all interviews. His role was to clarify language issues when needed. Each interviewer took written notes. In addition, the interviews were recorded. After each interview, each of the authors coded their notes. The notes were compared for consistency. We found close to 90% inter-rater agreement. Inconsistencies were resolved by listening to the recorded transcripts, consulting with the translator, and by follow up e-mails or phone conversations with respective interviewees. The final summaries were sent to each subject for their review and comments. If necessary, further phone calls or e-mails were used to clarify answers.

3.3 EDRM Projects

Company A considered and deployed EDRM within its organization mainly to achieve better control and security of proprietary knowledge within its organization (KMS). They plan to extend the use of EDRM projects in the near future.

Company B deployed EDRM essentially for securing and optimizing its e-Contracting processes with its extensive network of partners and subsidiaries (IOS). The major goals of the project were to secure documents (i.e., contracts) throughout their lifecycle and independent of their physical location at any given stage, prevent forgery, and help identify information leakage and leakage points. Future plans include full integration of EDRM among several processes and systems such as e-procurement and e-tax.

Company C deployed EDRM mainly in the scope of two projects. The first project is part of an enterprise wide centralized portal for the entire *chaebol* (involving over 40 companies and subsidiaries, and over 250,000 users worldwide.) The project mainly focused on email and attachments management. Company C had also gained additional insight into the implementation of EDRM through a document management project within a major government agency (this project was conducted on a consultancy/contract basis). Future implementation plans mainly focus on interoperability issues, expanding the rule-set to include additional content formats, and upgrading legacy infrastructures.

4. Results and Analysis

Tables 2 through 5 describe the general structure and operating environment of each organization, the importance placed on security (e.g., budgets, training), and the deployment of procedural and technical countermeasures.

Table 2. Operating Environment

Company	% of budget spent on security	Training	Critical factors	Comments
A	1.5%	Embedded in other processes	Securing sensitive information	Security is embedded in the culture
B	Not itemized	Included in overall employee training	Availability of information	
C	No break down	Included in over all employee training	Availability of information	Protecting proprietary (R&D) information is important

All three companies reported low employee turnover rate of about 5% and an average tenure of more than 15 years. This is especially important for the relative importance placed on content retirement such as the discontinuation of access privileges, the retirement of corporate equipment and documents accessed by ex-employees.

Table 3. Inter-Organizational Structure

Company	**Outsourcing**	**Contractors/ consultants**	**Remote workers and partners**	**comments**
A	No	Limited to large vendors	Sales and merchandizing, marketing and distributors	External entities do not have direct access to the back end systems; only to an image using company's issued equipment
B	No	No	Yes	20,000 partners involved with e-contracting
C	No	No	Occasional	Authorized personnel carry mobile devices (requires HQ approval). They have access only to their e-mail.

The three companies had implemented the traditional technical controls found in most large organizations such as firewalls, anti-virus and anti spam software, IDS, encryptions and access control mechanisms. Only company B is using biometrics for access control (Table 4).

Table 4. Technical Countermeasures

Company	**Anti Virus/spam**	**Firewalls**	**ACL**	**IDS/IDP**	**SSO**	**Biometrics**	**PKI**
A	Yes	Yes	Yes	Yes	No	Occasionally	No
B	Yes	Yes	Yes	Yes	Yes	Hand geometry	Yes
C	Yes	Yes	Yes	Yes	Yes	No. Due to users resistance	Yes

While the three companies have invested in most state-of-the-art technical controls, Table 5 indicates that there is little attention to business continuity, operational risk management and cyber insurance, among these companies.

Table 5. Procedural Countermeasures

Company	Business Continuity Planning	Operational Risk Management	Cyber insurance
A	Weak, not a major priority	Driven by K-SOX	No
B	Weak-planning a hot site by 2010	No	No
C	Hot sites	Yes	Partial-covers systems but not data

The three companies reported that they had experienced some security incidents in the 12 months prior to the interviews. Information leakage was cited to be a major issue. For example, around the time of this interview, there was a major private information breach in company C due to improper disposal of customers' statements. This breach was published in local papers but was not discussed specifically during the interview. However, most incidents are not reported since companies are not required to disclose when they are attacked. Company B reported less external incidents since they are not "as famous" as the other two companies, but stated that a major internal breach prompted them to implement their current EDRM solution. Their EDRM project appeared to be driven more by operational data management and control requirements than by high-level strategic objectives.

4.1 Ranking the Drivers

Towards the end of the interviews, we showed each company our three proposed drivers. The executives were asked to prioritize the drivers based on their importance for their respective company. The interviewees were also asked for their opinion as to the completeness of the set of drivers and to suggest additional potential drivers that they may have identified.

For company A, KM was ranked as the most important driver, followed by the other two, Compliance and IOS. The interviewees were unable to determine which of the two was more important. Concerning the completeness question, company A agreed that the three drivers represent a complete set and did not suggest any additional drivers.

Company B ranked IOS as the most important factor. This aligns with the company's extensive, external e-Contracting network supported by EDRM. Company B stated that KM is an adoption driver, although a weak one for now. Their plans are to integrate their KM systems with EDRM in the near future. Compliance ranked lowest as they claimed that they are "not really being involved with finance." As they assumed that compliance would be more salient for financial related companies. Company B did not suggest any additional driver either.

Company C proclaimed KM to be the major adoption driver. They ranked IOS far second. Since company C had very limited inter-organizational activity, the ranking was in reference to their general conceptualization of IOS and not specific to their organizational structure. Compliance ranked ~~the~~ third with minimal concern for the issue. Company C affirmed the set of drivers as complete. However, the interviewees mentioned "leakage prevention" as an additional adoption driver, referring to internal leakage of sensitive data. Leakage protection is an intrinsic security feature of EDRM since content can be managed even after leaving organizational boundaries.

5. THE EDRM MATURITY MATRIX

As mentioned above, while preparing the script for the interviews, we considered compliance as the leading driver behind organizational adoption of EDRM. To that end, we wanted to understand the relationships between compliance (i.e., legal requirements) and the expressiveness of the EDRM rule-set. Expressiveness refers to the richness of the rules, permissions and conditions enabled by the EDRM software. Expressiveness also refers to the granularity of the rule-set (i.e., file, record and item). The more expressive the EDRM rule-set, the more it aligns with organizational processes and structure. Therefore, as a part of the script, we prepared a 2X2 diagram with a legal dimension (whether binding or not) and a complexity dimension, denoting the complexity of the conditions and rights to be expressed (i.e., expressiveness power). Each quadrant represents one of four current readiness variables (i.e., the extent of industry's deployment of EDRM solutions in terms of legal binding and complexity of rights and conditions). The first quadrant (upper left) depicts the current state-of-affairs in the West (Morin and Pawlak 2007). EDRM solutions are driven by legal demands and contain relatively low expressiveness. The ultimate goal of EDRM is to support legal compliance combined with rich rule-set to support global, persistent content management (lower left quadrant). The upper and lower right quadrants depict mixed conditions. When the legal requirements are not binding and the complexity is low, EDRM is implemented as a proof-of-concept or a nice-to-have technology with limited business value. When the legal binding is low but the rule-set is rich and complex, the technology is adopted as an emerging technology or on a pilot basis. Each one of the three companies was shown the matrix depicted in Figure 1, and asked to position the company as of the day of the interview.

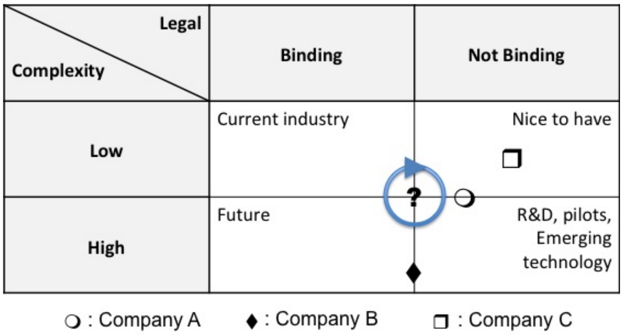
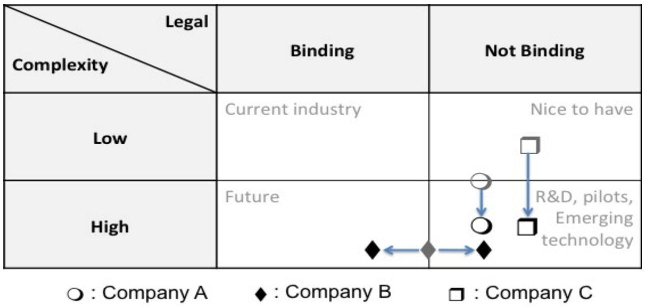


Figure 1. EDRM Maturity Matrix as of the Day of the Interview

Interestingly, we found that the three companies placed themselves in or at the border of the right side of the matrix (not legally binding). This is supported by our analysis of the interviews as described above.

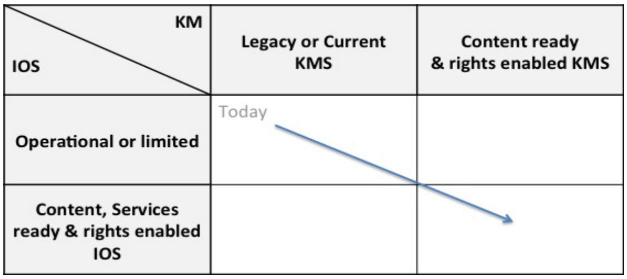
The executives were also asked to predict the company's position in the near future (1 to 3 years). This is reflected in Figure 2. Company A argued that they would stay on the right side of the matrix expecting to increase complexity (moving towards quadrant 4) but would not move towards increase in the legally binding dimension. This is because their internal company policies have higher standards than most current legal requirements. Company B positioned itself in the middle of the legal dimension in the high complexity bottom half of the matrix due to the complexity of their e-Contracting infrastructure. They expect that future implementations could lead them either way along the legal dimension depending on future legislations in the food industry. Company C positioned itself in the upper right quadrant expecting to move towards more complexity.



Legal / Complexity	Binding	Not Binding
Low	Current industry	Nice to have
High	Future	R&D, pilots, Emerging technology

Figure 2. EDRM Maturity Matrix Planed Evolution

While this EDRM Maturity Matrix needs to be refined and validated across industries, company size, and countries, we believe it could provide an interesting management tool for assessing and planning EDRM related projects. Similarly, considering the hypothesis that compliance could be embedded in sound KM and IOS readiness[7] (at least in the Korean context), we could imagine an alternative matrix in the following form (See Figure 3) with two dimensions: KM readiness and IOS readiness with indexes representing specific quantifiable functionalities of each. The upper left quadrant of the diagram describes the current implementations of KMS and IOS. The lower right quadrant indicates higher readiness for both aspects, namely, KMS supported by rich and advanced rights and policy management and IOS having strong cross-organizational services with rich and advanced rights and policy management. Given the view depicted in Figure 3, one can regard EDRM as an underlining technology that enables organizations to implement strong rights and policy management within and across organizations.



KM / IOS	Legacy or Current KMS	Content ready & rights enabled KMS
Operational or limited	Today	
Content, Services ready & rights enabled IOS		

Figure 3. KM-IOS Based EDRM Maturity Matrix

[7] This refers to the ability to design KM systems with compliance in mind (e.g., audit trails, strong security).

6. DISCUSSION

This exploratory study revealed several preliminary findings that need further investigation and validation. The key finding is that KM appears to be the primary driver for the implementation of EDRM in Korea. The three companies ranked KM as the highest priority. Companies A and C clearly identified KM as a top priority, while Company B acknowledged its importance.

Contrary to our initial assumption, it appears that compliance is not the most important driver behind organizational adoption of EDRM in South Korea. This appears to be contradictory to North American and European trends where many EDRM projects are driven by compliance related to Sarbanes-Oxley, Basel II, NASD 2711,[8] and HIPAA[9] (Morin and Pawlak 2007). This trend is also illustrated by the fact that majority of EDRM vendors' communication and marketing material is centered on compliance management (e.g., Liquid Machines[10]). Further research is needed to confirm these findings and to better understand the differences in adoption patterns across geopolitical regions.

One possible explanation for the above findings is the divergence between internal policies and external regulations among various countries. For Korean companies, internal policies appear to be much stronger than government mandates, while for Western companies mandates appear to be stricter than internal policies. In addition, corporate governance, recently under heavy scrutiny in corporate Korea (e.g., the Samsung case[11]), might be an interesting factor to consider in future studies. The historically strong ties between the Korean *chaebols* and the government (Lee 2009) may have also hindered corporate governance transparency. Therefore, Korean companies are driven by internal needs rather than by government regulations. This assertion is supported by the data collected during our interviews.

However, it is possible that the present evolution of corporate governance in Korea could lead to an increase in the importance of compliance in the future. The question then will be

[8] The National Association of Securities Dealers Rule 2711, filed by U.S. Security and Exchange Commissionaire in 2002.

[9] Health Insurance Portability and Accountability Act of 1996.

[10] Liquid Machines, Retrieved March 2009, http://www.liquidmachines.com/regulatory-compliance.

[11] Chairman of Samsung quits after indictment, Choe Sang-Hun, International Herald Tribune, Retrieved Feb 2009, http://www.iht.com/articles/2008/04/22/business/samsung.php.

whether the focus on non-compliance drivers have helped address future increase in corporate governance issues. Such a change might also result in an entirely different “future” than is depicted in the planned evolution of Figure 2.

Finally, following the adage that “what can do the most, can do the least,” a sound Knowledge Management approach to organizational information and knowledge assets could result in the organization’s ability to address compliance management. A technical infra-structure allowing tracking, monitoring, auditing and governing content throughout the organization’s structure and processes would result in inherent compliance.

The three cases explain the adoption pattern of EDRM in South Korea and illustrate the readiness and maturity level of organizational corporate information and knowledge assets and the strategic value these organizations place on these systems.

These issues will, in our opinion, become increasingly important as we progress towards materialization of the extended virtual enterprise and its corresponding challenges. In other words, one could assert that compliance is a consequence of KM and IOS ready organizations. In which case, KM and IOS readiness in terms of maturity level could represent a valuable indicator for organizations to assess and plan their infrastructure and organizational development. This is further supported by the advancement towards “cloud computing” (Buyya et al. 2009). Cloud computing integrates IOS and KMS into a highly commoditized infrastructure (including software and data) used to deliver as services to organizations. To participate in the “cloud,” organizations are expected to have high levels of readiness in areas such as content management policies, access management, and rules governing the use of information assets across organizational boundaries-all can be facilitated by EDRM.

7. CONCLUSION AND FUTURE WORK

This study is part of an ongoing large-scale project. Due to the novelty of the technology, we opted to begin our investigation by conducting an in-depth case study. The case studies underscore the strategic importance of KM and IOS while deemphasizing the importance of regulatory compliance in the context of EDRM adoption by large South Korean companies.

In the next phase of the project, we will attempt to validate our findings through a large-scale survey of companies in South Korea, North America, and Europe. We expect this project to help us further understand organizational adoption of EDRM and its major drivers. In addition, our goal is to further characterize the business value of EDRM and provide justifiable elements for investments in EDRM projects.

Finally, we expect to develop the EDRM Maturity Matrix as an assessment and planning tool for organizations wishing to explore the deployment of EDRM and thus increasing awareness of the strategic nature of EDRM throughout the extended virtual organization.

ACKNOWLEDGEMENTS

We would like to extend our warm thanks to Dr. K. Cho, CEO and to Ms. V. Kim, Senior Marketing Manager of Fasoo.com, for their help in making this study possible. Our appreciation also goes to the respective people within the three organizations who kindly accepted to participate in this study and to Mr. Jaewoo Joo who assisted in the interview process by providing clarification on English-Korean language aspects of the survey.

REFERENCES

Buyya R, Yeo CS, Venugopal S, Broberg J, & Brandic I (2009) Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems 25(6):599-616.

D’Arcy J, Hovav A (2007) Deterring Internal Information Systems Misuse. Communi-cations of the ACM 50(10):113-117.

D’Arcy J, Hovav A, & Galletta, D (2009) User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 20(1):79-98.

Davenport T, Prusak L (1998) Working Knowledge. Harvard Business School Press. Boston, MA.

Eisenhardt K (1989) Building theories from case study research. Academy of Management Review 14(4):532-550

Fasoo (2008) Fasoo, company web site, retrieved, April 2008. http://www.fasoo.com/ Accessed 2012-06-15.

Fichman RG. Kemerer CF (1993) Adoption of software engineering process innovations: The case of object orientation. Sloan Management Review 34:7-22.

Hovav A. Berger R (2009) Identity Management Systems and Secured Access Control. Communications of the AIS, 25(1):531-570.

Jaruzelski B, Dehoff D (2008) *Beyond Boarders: The Global Innovation 1000.* Strategy+ Business 53 (Winter).

Lee KS (2009) A final flowering of the developmental state: the IT policy experiment of the Korean Information Infrastructure, 1995-2005. Government Information Quarterly 26 (4):567-576

Morin JH, Pawlak M (2007) From Digital Rights Management to Enterprise Rights and Policy Management: Challenges and Opportunities. In: Herrmann F, & Khadraoui D (Eds) Advances in Enterprise Information Technology Security, Information Science Reference, IGI Global, Hershey, PA:169-188.

Morin JH (2008) Exception Based Enterprise Rights Management: Towards a Paradigm Shift in Information Security and Policy Management. International Journal on Advances in Systems and Measurements 1(1):40-49.

Morin JH (2009) Rethinking DRM Using Exception Management. In: Lian S, & Zhang Y (Eds) Handbook of Research on Secure Multimedia Distribution, Information Science Reference, IGI Global, Hershey, PA, 39-54.

Rogers EM (1983) Diffusion of Innovations. 2nd Ed. The Free Press. New York, NY.

Sambamurthy V (2000) Business strategy in hypercompetitive environments: rethinking the logic of IT differentiation. In: Zmud RW (Ed) Framing the Domains of IT Management, Pinnaflex Educational Resources, Cincinnati, OH:245-261.

Tarantino A (2008). The Governance, Risk, and Compliance Handbook: Technology, Finance, Environmental, and International Guidance and Best Practices. John Wiley and Sons, Inc. New York, NY.

Yin RK (1994) Case Study Research Design and Methods. Sage Publications. Thousand Oaks, CA.

<APPENDIX A> Interview Script Sample

IOS:

1. Does the organization have a need for security management across organizational boundaries?
2. How does the organization handle security issues for each of the following external stakeholders
    - Outsourcing/hosting
    - Off-shoring
    - Contractors
    - Consultants
    - Auditors
    - Telecommuting
    - Remote/mobile workers
    - Partners with access to company information
    - Partners with access to company Intranet (Extranets)
3. Do any of these entities have access rights to organizational information?
4. Is there a need for dynamic assignments of rights, if so when and how are they being handled?
5. Are employees allowed to physically carry information out of the organization?
6. Are employees allowed to electronically carry information out of the organization?
7. Are employees allowed to electronically send information to external entities?
8. Are employees allowed to store data externally?
9. Do you require real time connectivity?

Disposal of hardware and content

1. What procedures are used to dispose of hardware?
2. What procedures are used to dispose of electronic content?
3. Are these procedures implemented both in the organization and externally?

Access to systems

1. How do you handle employees who leave the company/new employees: Processes for de-commissioning (revocation, etc.)/granting etc. (number of systems they have access to)

Knowledge Management:

1. How would you define knowledge in your organization?
2. How is that knowledge managed?
3. What type of organization we are studying?
   A. Level of sensitivity of data
   B. How many knowledge workers do you have (proportion %)
   C. In what capacity are these employees used for?
4. What is the level of sophistication of the employees (for each, level of education)?
   A. Consultants
   B. Engineers
   C. Financial advisers
   D. Clerical employees
   E. Middle Managers
   F. Managers (senior)
5. Do you have data classification scheme? (Specify for each: email, internal communication, communication with the outside, documents, design, strategic/financial planning, Enterprise applications outputs, other …)
   A. If so, what is it?
   B. If it uses a DRM solution, how was it managed before?
   C. How is it managed now?
6. Do you have retention policies?
   A. If so, what are they? (Specify for each: email, internal communication, communiaion with the outside, documents, design, strategic/financial planning, Enterprise applications outputs, other …)

   B. If it uses a DRM solution, how were they managed before?
   C. How are they managed now?
   D. How do you handle legacy (old) digital media?

7. Do the employees have access to:
   A. Private data
   B. Trade secrets
   C. R&D data/CAD content
   D. Financial data
   E. Embargoed information (limited access prior to a given event)
8. What will be the consequences if employees divulge that information?
   A. For employees
   B. For management
   C. For the company
      i. Brand name damage
      ii. Liability
      iii. Trustworthiness

Legal, Policy and Regulatory Compliance:

- Does your company have a Chief Compliance Officer (CCO)? If yes, what are his quailfications?
- Does your company have internal controls?
- Does your company go through external auditing processes? Entity performing the audits?
- Is your company concerned with Operational Risk Management? If yes, what has been enforced in ORM?
- How concerned is your company with the following :
  - Data protection (e.g., classification, identification, encryption, traceability)
  - Legal and regulatory compliance
  - Leakage of private information (proprietary information, IP, trade and business secrets, patents, design CAD documents, etc.

  - Security awareness training and other education initiatives
- How do you feel about the following statements :
  - Legal and regulatory compliance has raised my organization’s level of interest in information security
  - Legal and regulatory compliance has changed the focus of information security in my organization from technology to one of corporate governance.
  - Unintentional incidents (e.g., unintentional misuse) occur more often than intentional incidents (e.g., accidental leakage, etc.)
  - Security is about achieving a commercially viable risk level while allowing operations to run smoothly
  - Assuming a digitally enabled policy management infrastructure, it would be seen as a help rather than a constraint
  - Assuming a secure and digitally enabled policy management infrastructure, incidents would have a better chance of being intentional
- What is the regulatory environment of the organization? Which regulation the company has to comply with?
  - National
  - Global
- Do you have Industry related business practices and policies that must be enforced? Elaborate?
- Do you have Industry related standards that must be enforced? Elaborate?
- Do you have internal policies and rules that must be enforced? Elaborate?

- What is required by law in terms of?
  1. Privacy
  2. Maintenance of digital information-what has to be kept, for how long, in what format?
  3. Is audit trail required?
  4. What is supposed to be captured in the audit trail?
  5. What are the penalties associated with non-compliance?

6. Is the organization liable for partners, contractors and other related entities that do work for the organization?

- What is required by the organization’s corporate rules and policies?
   1. Privacy
   2. Maintenance of digital information-what has to be kept, for how long, in what format?
   3. Is audit trail required?
   4. What is supposed to be captured in the audit trail?
   5. What are the penalties associated with non-compliance?
   6. Is the organization liable for partners, contractors and other related entities that do work for the organization?
- Is tracking and monitoring important for your organization? (How do you balance between privacy and monitoring?)

AUTHOR BIOGRAPHY

Jean-Henry Morin is Associate Professor of Information Systems and Services at University of Geneva, Faculty of Economic and Social Sciences. Member of the Institute of Services Science he is also program director of the Bachelor in Information Systems and Services Science and president of ThinkServices, a Think Tank on Services Science and Innovation where he leads an interdisciplinary group who recently launched ThinkData.ch an awareness service on data protection and transparency. He was Associate Professor at Korea University Business School in Seoul until 2008. He is co-founder and advisory board member of PebbleAge, a Geneva based company specialized in corporate performance management solutions where he was director of research and development and led an Enterprise DRM business unit until 2004. He holds a PhD and an MSc in Information Systems from University of Geneva. His research interests include Digital Rights and Policy Management (DRM/DPM), exception management in DRM environments, IS security, green security (socially responsible and sustainable security), corporate information asset management, governance, risk and compliance (GRC), data protection and privacy, electronic commerce and services, Peer-to-Peer computing, cloud computing, mobile objects (agents), IoT, electronic publishing and information services over open networks.

Dr. Anat Hovav is a professor of MIS at Korea University Business School in Seoul, South Korea. Her research interests include the socio-technical aspects of organizational information security, risk assessment, emergent technology and innovation management, and electronic scholarship. Anat Hovav has published in internationally refereed journals such as: Information Systems Research (ISR), Information and Management, Communications of the ACM, Journal of Business Ethics, Research Policy, Computers and Security, Information Systems Journal (ISJ), Information Systems Management (ISM), Communications of AIS (CAIS), Information Systems Frontiers, and Risk Management and Insurance Review.